Chapter 6
Aerodrome Security

The airport is the frontier between the outside world and the State in which the airline passenger lands. It is also the final point at which a person can be checked before embarking on a flight. Moreover, the aerodrome is where cargo is loaded into an aircraft before takeoff. Therefore, security at the airport carries multiple dimensions, from border control to body scanning; from cargo security to security of the aircraft and its passengers.

Encouragingly, information technology assists in ensuring aerodrome security and overall airport operations. Facilities such as online check-in where airlines can check in passengers through their mobile services, ease congestion at the terminal check in counters; mobile devices and hand held terminals with Wi-Fi connections; biometric technology and passenger tracking technologies all go to ensure a more efficient and secure airport operation. Pilots and aircrew have *i*Pads and other tablets to deliver critical information and data; and passengers have smart phone apps top report any suspicious behaviour in their vicinity.

6.1 Border Security

Article 22 of the Chicago Convention states that each contracting State agrees to adopt all practicable measures, through the issuance of special regulations or otherwise, to facilitate and expedite navigation by aircraft between the territories of contracting States, and to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially in the administration of the laws relating to immigration, quarantine, customs and clearance. This provision is followed by Article 23 which provides that each contracting State undertakes, so far as it may find practicable, to establish customs and immigration procedures affecting international air navigation in accordance with the practices which may be established or recommended from time to time, pursuant to this Convention.

The fundamental requirement in the immigration process is the passport. One of the key aspects of facilitation involves speedy, efficient and secure border crossing.

R. Abeyratne, *Law and Regulation of Aerodromes*, DOI 10.1007/978-3-319-04780-5_6,

The primary tool for this process is a valid travel document. A discussion of passports and visas has already take place in this book under Article 13. However, there remains one aspect to be discussed and that is State responsibility in protecting the integrity of the passport and the prevention of passport fraud.

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 assassination of a leader of Hamas on 19 January 2010 by a group of individuals in Dubai who used forged passports belonging to various nations, raised a diplomatic outcry and brought to bear an important facet of air transport that is vulnerable to abuse and contention among States.

The fundamental issue that emerges is one that is critical to air law in the context of the integrity and ownership of the passport and its abuse in the course of criminal activity. There is also the issue, from a legal and diplomatic perspective as to whether a State or instrumentality of State, can, with impunity, use forged passports for travel of its staff on missions of espionage or assassination. *A fortiori*, an additional issue is whether a State could be complicit or condone or be seen to condone (in the absence of any action taken by the State to punish the miscreants) such abuse of travel documents belonging to other nations. In order to determine these issues, this article addresses two basic discussions: the first on complicity and condonation of a State and the second on the nature and integrity of the passport. Finally, it discusses issues of State responsibility, diplomacy and criminality.

On 19 January 2010, Mahmoud al-Mabhouh, considered to be a senior commander of Hamas, a radical Palestinian group, was assassinated at a hotel in Dubai in a manner usually employed by professionally trained military and secret service agencies. The killing was attributed to Mossad[1] The European Union, which considers Hamas a terrorist organization, nonetheless condemned the assassination of the Hamas leader and showed particular concern over the fact that the killers had used passports from Ireland, France, Germany and the UK—to coordinate their travel into Dubai from various parts of the world, synchronizing their arrival time from various flights into Dubai International Airport and checking into the hotel of the victim contemporaneously. The EU strongly condemned the fact that those involved in this action used fraudulent EU member states' passports and credit cards acquired through the theft of EU citizens' identities.[2]

Australia was another complainant who warned Israel that its friendly relations with Israel would be jeopardised if it were found to have condoned the suspected

[1] Mossad is responsible for the collection of intelligence and other covert activities including military operations. It is one of the most integral parts of the Israeli intelligence community and reports directly to the Prime Minister of Israel. See http://en.wikipedia.org/wiki/Mossad.

[2] Toby Vogel, EU Condemns Use of False Passports inn Hamas Killing, http://www.europeanvoice.com/article/2010/02/eu-condemns-use-of-false-passports-in-hamas-killing/67225.aspx.

theft of three Australian citizens' identities which Mossad used to carry out its political assassination. The diplomatic impasse occurred when three Australians from Victoria living in Israel at the time were confirmed among 26 people from four nations whose tampered passports were allegedly used by a team of suspected Israeli Mossad agents who assassinated al-Mabhouh. Australian Prime Minister Kevin Rudd is reported to have stated that Australia would be vocal in its contempt of any State if it were found that it ". . . has been complicit in the use or abuse of the Australian passport system, let alone for the conduct of an assassination, and has treated Australia with contempt and there will therefore be action by the Australian government in response".[3] Dubai authorities are reported to have said that they were virtually certain Israeli agents carried out the killing and had released the identities of 11 people who travelled on forged British, Irish, French and German passports to kill al-Mabhouh in a hotel.[4]

There is seemingly a history behind alleged Mossad involvement in the use of fake foreign passports in its activities. Reportedly, in 2004 New Zealand's prime minister imposed diplomatic sanctions—restricting visas and cancelling high level visits—after two Mossad agents were caught trying to acquire passports fraudulently—one in the name of a tetraplegic man. Seven years earlier, Mossad assassins carrying Canadian passports with assumed names attempted to murder the Hamas leader Khaled Meshaal by spraying nerve agent into his ear as he entered his office in Amman.[5]

The fundamental issue that emerges is one that is critical to air law in the context of the integrity and ownership of the passport and its abuse in criminal activity. There is also the issue, from a legal and diplomatic perspective is whether a State or instrumentality of State such as Mossad, can, with impunity, use forged passports for travel of its staff on missions of espionage or assassination. *A fortiori*, an additional issue is whether a State could be complicit or condone or be seen to

[3] http://www.theaustralian.com.au/news/world/australians-caught-in-hit-on-hamas/story-e6frg6so-1225834538825. It is reported that in 1997, Mossad bungled the assassination of top Hamas leader Khalid Mishal, who was injected while in Jordan with a poison by Israeli agents travelling on Canadian documents. He survived after his assailants were captured by his bodyguards and Israel provided the antidote. In 2004, two Mossad agents were jailed in New Zealand after trying to obtain fake passports, one in the name of a cerebral palsy sufferer. *Ibid.*

[4] http://www.euractiv.com/en/foreign-affairs/eu-unhappy-israel-over-fake-passports-james-bond-killings-news-278602.

[5] David Sapsted, and Loveday Morris, Israel in the Dock Over Fake Passports, http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100218/NATIONAL/702179796/1133/sport.
Hamas, which won 2006 legislative elections in the Palestinian territories, is shunned by the West for rejecting its calls to recognise Israel and renounce violence. Hit squads dispatched by Mossad have used foreign passports in the past, notably in 1997 when agents entered Jordan on Canadian passports and bungled an attempt to kill Meshaal with poison. In 1987, Britain protested to Israel about what London called the misuse by Israeli authorities of forged British passports and said it received assurances steps had been taken to prevent future occurrences. In 2003, the offices of several EU member countries in the Council's Justus Lipsius building, including France, Germany and the UK, were found to be bugged. Although the Union has been discrete over the incident, many consider Mossad to have been responsible for the wiretapping. *Ibid.*

condone (in the absence of any action taken by the State to punish the miscreants) such abuse of travel documents belonging to other nations.

6.1.1 The e-Passport

Starting from the premise that the passport is primarily a document which establishes the identity of the holder,[6] the various approaches[7] taken by ICAO in advancing technologies that facilitate this task at borders have evolved into the use of biometric identification of the passport holder as the ultimate frontier in the identification process. The techniques of biometrics employed in a machine readable travel document (MRTD), be it a visa or passport,[8] enable the user to uniquely encode a particular physical characteristic of a person into a biometric identifier or biometric template which can be verified by machine to confirm or deny a claim regarding a person's identity. Accordingly, biometric identification of a person either correctly establishes his identity as being consistent with what is claimed in the passport he is holding or brings to bear the possibility that the person carrying a particular passport is an imposter. A biometric is a measurable, physical

[6] See *Naziranbai* v. *the State*, 1957 *Madhya Bharat Law Reporter*, at 1, where the court recognized the passport as essentially being a document of identity and nationality issued to citizens or subjects of a state who intend to travel overseas. See also, Turack (1972) at 20–21. Also, Abeyratne (1992) at 10.

[7] 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. See Facilitation Division, Report of the Seventh Session, 14–30 May 1968, ICAO Doc 8750-FAL/564, Agenda Item 2.3, at 2.3-4. See also *AT-WP/1079, 1/12/70*, Attachment A, which sets out the Terms of Reference of the Panel.

[8] A passport asserts that the person holding the passport is a citizen of the issuing State while a visa confirms that the State issuing the visa has granted the visa holder the non-citizen privilege of entering and remaining in the territory of the issuing State for a specified time and purpose. 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. Abeyratne (1992), pp. 1–31.

characteristic or personal behavioral trait used to recognize the identity, or verify[9] the claimed identity of a person. In the modern context, biometrics are usually incorporated in an MRTD with a view to achieving five goals, the first of which is global interoperability[10] enabling the specifications of biometrics deployed in travel documents across the world to be applied and used in a universally operable manner. This is a critical need if the smooth application of biometric technology were to be ensured across borders. The second goal is to ensure uniformity within States in specific standard setting by States authorities who deploy biometrics in travel documents issued by them. The third is technical reliability, where States are required to ensure that technologies used in deploying biometrics are largely failure-proof and of sufficient quality and standard to ensure a State immigration authority reading documents issued by other States them that the details in the document do provide accurate verification of facts. Fourthly, the technology used has to be practical and not give rise to the need for applying disparate types of support technology at unnecessary cost and inconvenience to the user. The final goal is to ensure that the technology used will be sufficiently up to date for at least 10 years and also be backwardly compatible with new techniques to be introduced in the future.

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[11] of a State and when the State verifies his identity against the images or templates created at the time his travel document was issued.

[9] 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.

[10] "Global interoperability" means the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective states. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine-readable data in all MRTDs.

[11] The Chicago Convention, *supra*, 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.

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)[12] 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.[13] 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.

In May 2003, The New Technologies Working Group (NTWG) of the Technical Advisory group on Machine Readable Travel Documents (TAG/MTRTD) of ICAO, endorsed its *New Orleans Principle* of March 2003, which resolved that member States will continue to use the facial image as the primary identifier for MRTDs and as such the utilization of standardized digitally-stored facial images should be the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with MRTDs. Furthermore, the NTWG recognized that in addition to digitally stored facial images, member States of ICAO could also use digitally stored iris images or fingerprints as additional globally interoperable biometrics for purposes of identifying persons through MRTDs.

The challenges facing biometric technology are few, but significant. Biometric technology is evolving so rapidly that it is difficult to maintain consistent standards. The standards themselves are not regularly tested. Some technologies are not

[12] 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), pp. 631–650.

[13] 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.

adequately established so as to lend themselves to easy decoding and interpretation, particularly when confirming identity on a one-to-one basis with a large central database. More importantly, from a legal perspective, biometric technology brings to bear the compelling need to be aware of privacy issues[14] and data protection legislation of various jurisdictions, as well as liability of the database manager that might emerge pursuant to a breakdown of the database or inaccuracy of information produced as a result of data-matching, which in turn might lead to inconsistencies in the identification process.

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 ICAO in early October 2012, the ePassport was subjected to much discussion by the various experts gathered from across the globe.

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 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". 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 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

[14] Abeyratne (2001), pp. 153–162. Abeyratne (2002b), pp. 83–115. Also Abeyratne (2002a), pp. 631–650.

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) 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 determination is effected, where the digitized photograph is visually matched (non electronically) with the three way check described above. 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.

6.1.2 Passenger Name Record

One of the most dramatic events pertaining to aviation security occurred in July 2005 when United States air traffic controllers turned back a KLM flight en route to Mexico City from Amsterdam, which was flying over US airspace. The action was grounded on the basis that two of the passengers in the passenger list earlier provided to the US authorities were on a "no fly" list. The importance of this drama to modern day aviation is that the aircraft was merely over-flying the territory of a State. Even more important is the fact that at the time of the incident, there was no US legislation covering the act of refusal to grant over-flying permission to an aircraft in that situation.[15] However, within days, The US Transportation Security Administration (TSA) announced that rules will be adopted to require that

[15] Consequent upon the events of 2001, President George Bush signed a new *American Transportation & Security Act* on November 25th 2002 making mandatory API transmission and the provision of PNR data pertaining to all passengers arriving in the United States. Such information, required prior to departure and arrival in the United States should include in the passenger and crew manifest for each flight, in accordance with, Section 115 of the *Transportation & Security Act* is

(a) The full name of each passenger and crew member;
(b) The date of birth and citizenship of each passenger and crew member;
(c) The sex of each passenger and crew member;
(d) The passport number and country of issuance of each passenger and crew member if required for travel;
(e) The United States visa number or resident alien card number of each passenger and crew member, as applicable;
(f) Such other information as the under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety.

passengers on all flights landing in and overflying US territory will be screened against a "no fly" list.[16]

The Passenger Name Record (PNR) is a subject that has been under intense scrutiny by the Council of ICAO which has developed PNR Data Guidelines that have been transmitted to Contracting States for their comments[17] This exercise was carried out on the understanding that, in the present context of the compelling need for the enhancement of aviation security, the global aviation community has shown an increased interest[18] in adding the PNR data as a security measure in addition to the already existing Advanced Passenger Information (API)[19] and the Machine Readable Travel Document (MRTD), which, although primarily are facilitation tools, greatly assist States authorities in ensuring border security.

One of the issues that emerge from PNR data collection is extraterritoriality and the question as to whether at law a State can require information held by other States relating to flights that originate and end in the latter States. An example is Canada, which may be required by the US to divulge information pertaining to passengers on domestic flights operating within the territorial limits of Canada but over-fly United States' territory for reasons of expediency and fuel efficiency. While there is no room for doubt that usually, requirements for safety and security of a State are based on sound legal justification with a view to protecting A State's integrity and internal security, a requirement for information by a particular State of those that do not enter the territory of that State might open itself to question, as to whether such would impinge upon another sovereign State's right to privacy[20] and dignity.

A Recommended Practice for inclusion in Annex 9 to the Chicago Convention (Facilitation) was adopted by the ICAO Council in March 2005. This Recommended Practice, which supplements an already existing Recommended

[16] Crossing the Line, *Airline Business*, August 2005, at 9.

[17] Attachment to State Letter EC 6/2-05/70, Passenger Name Record (PNR) data, 9 June 2005.

[18] The advantage of collection by States of PNR Data was first discussed by the global aviation community at the 12th Session of the ICAO Facilitation Division that was held in Cairo, Egypt from 22 March to 1 April 2004. Consequently, the Division adopted Recommendation B/5, that reads as follows:

> It is recommended that ICAO develop guidance material for those States that may require access to Passenger Name Record (PNR) data to supplement identification data received through an API system, including guidelines for distribution, use and storage of data and a composite list of data elements [that] may be transferred between the operator and the receiving State.

Pursuant to this recommendation, In June 2004, the Air Transport Committee of the ICAO Council requested the Secretary General to establish a Secretariat Study Group to develop Guidelines on PNR data transfer. The Council, in endorsing Recommendation B/5, directed that these Guidelines were to be submitted early in 2005.

[19] See Abeyratne (2002a), pp. 631–650. Also Abeyratne (2001), pp. 153–162, and also by Abeyratne (2003), pp. 297–311.

[20] See Abeyratne (2001).

Practice, provides that Contracting States requiring Passenger Name Record (PNR) access should conform their data requirements and their handling of such data to guidelines developed by ICAO. It is worthy of note that Article 13 of the Chicago Convention provides that 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. This provision gives a State the discretion to specify the information it requires relating to persons wishing to gain entry into its territory. Accordingly, a State may require aircraft operators operating flights to, from or in transit through airports within its territory to provide its public authorities, upon request, with information on passengers such as PNR data.

The philosophy underlying the importance of PNR data and their efficient use by States for enhanced expediency in border crossing by persons is embodied in, the General Principles set out in Chapter 1 of Annex 9 which require Contracting States to take necessary measures to ensure that: the time required for the accomplishment of border controls in respect of persons is kept to the minimum[21]; the application of administrative and control requirements causes minimum inconvenience; exchange of relevant information between Contracting States, operators and airports is fostered and promoted to the greatest extent possible; and, optimal levels of security, and compliance with the law, are attained.

Contracting States are also required to develop effective information technology to increase the efficiency and effectiveness of their procedures at airports[22]

6.1.3 Definition and Application of PNR

The air transport industry regards a Passenger *Name Record* (PNR), as a, generic term applicable to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. The data is used by operators for their own commercial and operational purposes in providing air

[21] There is an abiding symbiosis between security and facilitation in the field of air transport. While security is of paramount interest to the global aviation community, it must not unduly disrupt or in any adversely affect the expediency of air transport. To this end, Recommended Practice 2.2 of Annex 9—Facilitation—to the Chicago Convention suggests that Each Contracting State should whenever possible arrange for security controls and procedures to cause a minimum of interference with, or delay to the activities of civil aviation provided the effectiveness of these controls and procedures is not compromised. See McMunn (1996) at 7.

[22] It must be noted that Annex 9 specifies that the provisions of the Annex shall not preclude the application of national legislation with regard to aviation security measures or other necessary controls.

transportation services.[23] The definition applicable in the United States identifies a PNR as a repository of information that air carriers would need to make available upon request under existing regulations and refers to reservation information contained in a carrier's electronic computer reservation system[24]

The above definitions and identifiers go to show that a PNR is developed and constructed from data that has been provided by or on behalf of the passenger concerning all the flight segments of a journey.[25] This data may be added to by the operator or his authorized agent, for example, changes to requested seating, special meals, additional services requested, *etc*. PNR data could be obtained in many ways. For example, information captured through reservations created by international sales organizations (global distribution systems "GDS" or computer reservation systems "CRS") with pertinent details of the PNR could be transmitted to the operating carrier(s). When reservations are made directly by the aircraft operator and the complete PNR is stored within the operator's automated reservations systems, the information therein could be a useful repository of PNR data. Information contained in records of some operators who may hold sub-sets of the PNR data within their own automated departure control systems (DCS), for their information or for onward transmittal to contracted ground handling service providers, calculated to support airport check-in functions would be another way in which PNR data could be provided. However, it must be noted that in each case, operators (or their authorized agents) will have access to, and be able to amend only that data that has been provided to their system(s). An important consideration in this regard is that some DCS systems are programmed such that details emerging from check-in (i.e. seat and/or baggage information) can be overlaid into the existing PNR for each passenger. However, that capability is limited—covering less than 50 % of operating systems today.

The time element, with regard to the capture and relevance of PNR data, is relevant to the use of such data. For instance, Data could be entered into a reservation system many days or weeks in advance of a flight. This could extend to as long as 345 days in advance of departure. Under such circumstances, both the provider and the receiver of PNR data must bear in mind that Information in reservation systems is dynamic and may change continuously from the time when the flight is open for booking. On the other hand, passenger and flight information in the DCS, becomes available only from the time the flight is "open" for check-in

[23] The Industry Standards related to PNR creation are detailed in IATA's *Passenger Services Conference Resolutions* and in the ATA/IATA *Reservations Interline Message Procedures (AIRIMP) Manual*.

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

[25] There are two possible methods of PNR data transfer currently available: (a) the "pull" method, under which the public authorities from the State requiring the data can reach into the aircraft operator's system and extract ("pull") a copy of the required data into their database; and (b) the "push" method, under which aircraft operators transmit ("push") the required PNR data elements into the database of the authority requesting them.

(up to 48 h prior to departure). In such an instance, departure control information for a flight will be finalized only upon flight closure, and may remain available 12–24 h after arrival of a flight at its final destination.

In the case of aircraft operators specializing in charter air services, who often do not hold PNR data in an electronic form, but still use a DCS which will only enable them to have a limited PNR record after the flight has closed, they would still be required to provide any captured data to States requesting it regardless of the process by which they receive PNR data. States could also require supplemental or "requested service" information which may be contained in the PNR, such as information relating to special dietary and medical requirements, "unaccompanied minor" information, requests for assistance etc.

Operators should take particular care in refraining from incorporating in PNR data any information that is not essential to facilitate the passenger's travel. Such information would include, but not be necessarily restricted to details of the passenger's racial or ethnic origin, political opinions, religious or political beliefs, trade-union membership, marital status or data relating to a person's sexual orientation. The ICAO guidelines make specific mention of the fact that Contracting States should not require aircraft operators to collect such data in their PNRs.

The above notwithstanding, any information which would legitimately facilitate the carriage of the passenger, such as details of meal preferences and health issues as well as free text and general remarks, could comprise the PNR. Sensitive data contained in the PNR and is submitted in compliance with a regulation of a State should not be used as the primary source for assessment of risk that the passenger might present to the State concerned.

6.1.4 The Importance of PNR Data to States

From a regulatory perspective, the two main areas to which PNR data make a contribution are expedition of customs and immigration processing at airports; and facilitation of passenger traffic and the safeguard of the legitimate rights of the passenger. The Chicago Convention provides a sound basis for States to require PNR data in the current context. The Convention, in Article 22, recognizes the importance of facilitating the passage of a person through borders by requiring each contracting State to adopt all practicable measures, through the issuance of special regulations or otherwise, to facilitate and expedite navigation by aircraft between the territories of contracting States, and to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially the administration of the laws relating to immigration, quarantine, customs and clearance.

The main reason for States to require the advance submission of PNR data is that such data could prove to be a valuable tool in ensuring aviation security. PNR data are critically important for the threat assessment value that can be derived from the analysis of such data, not only in possible instances of unlawful interference with civil aviation but also in relation to the fight against terrorism. This critical value of

PNR data has prompted some States to enact legislation or develop draft legislation for approval by their Legislatures requiring that aircraft operators provide their public authorities with PNR data.

PNR data primarily enable States, through the identification of potentially high-risk passengers through PNR data analysis, to improve aviation security; enhance national and border security; prevent and combat terrorist acts and related crimes and other serious crimes that are transnational in nature, including organized crime; and to enforce warrants and prevent flight from custody for such crimes. Such data could also protect the vital interests of passengers and the general public, including their health.

States are aware that, if the guidelines are implemented in a uniform manner, would provide a global framework enabling all States to benefit from the value-added analysis of PNR data for shared security/safety purposes. Air carriers would also benefit from having to comply with only one set of common requirements for PNR data transfer. As for the consumer of air transport, all passengers would o benefit from basic protection afforded to them by the exchange of PNR data between air carriers and State authorities.

The above notwithstanding, there are certain fundamental obligations that the State receiving the data has to fulfill. Firstly, States should require PNR data only of those passengers on flights that are scheduled to enter, depart or transit through airports situated in their territories. Secondly, a State obtaining PNR information should, as a minimum limit the use of data to the purpose for which it collects it. States must restrict access to such data, ensure that the data is adequately protected, and limit the period of data storage, consistent with the purposes for which data is transferred. States must also ensure that individuals are able to request disclosure of the data that is held on them, consistent with the guidelines, in order to request corrections or notations, if necessary. More importantly, they must ensure that individuals aggrieved by the PNR data collection and usage process have an opportunity for redress.

The responsibility of ensuring that their public authorities have the appropriate legal authority to process PNR data requested from aircraft operators, in a manner that observes the guidelines, devolves entirely upon the States. They have been requested by ICAO to forward the full texts of legislation pertaining to PNR data dissemination and use to ICAO for online dissemination to other States, for information. The State concerned will be responsible for responding to any queries arising from such legislation.

6.1.5 Advantages of Unified Guidelines

Through the PNR Data Guidelines ICAO has introduced uniform measures for PNR data transfer and the subsequent handling of that data by the States concerned. The guidelines are both durable and easy to follow, making them cost effective for the parties concerned. They would ensure accuracy of information, while at the same

time protecting the data subject against encroachment of his privacy. The Guidelines call for completeness of data and the need for timely submissions and effective collection of data. They also ensure that data management will be efficient and efficacious. From a practical perspective, the guidelines also provide useful directions assisting States in designing data requirements and procedures, in order to minimize technical difficulties that might prove too onerous and may impair the implementation of the uniform measures suggested. The Guidelines also contain detailed instructions with a view to assisting both air carriers and States on PNR data transfer from an operator's system to a State and the management of the data including arrangements for storage and protection.

States are enabled, by the guidelines, to design systems and establish arrangements that are compatible with the guidelines while not impairing their ability to implement their laws and enforce them. The guidelines do not interfere with the preservation of national security and public safety of a State. Arguably, one of the most important features of the unified PNR data guidelines is that, by their very nature, they would effectively obviate the complexities that aircraft operators could face with regard to legal, technical and financial issues if they were to be required to respond to multiple, unilaterally imposed or bilaterally agreed PNR data transfer requirements that differ substantially from one another.

States also have the responsibility of enacting explicit legal provisions concerning data transfer. Such legislation should clearly elaborate on the reasons for requiring PNR data, or provide explanatory material accompanying such laws or regulations, as appropriate. Since an aircraft operator is obliged to comply with the laws of both the State from which it transports passengers (State of departure) and the State to which these passengers are transported (destination State), when a destination State legislates with regard to its PNR data transfer requirements, it should do so cognizant of the fact that *existing* laws of other States may affect operators' ability to comply with these requirements. Therefore, where there could be an inconsistency between two legal regimes of the departure State and the destination State, or where a conflict arises between any two States, or where an operator advises of a conflict, The ICAO guidelines suggest that the States involved should consult each other to determine what might be done to enable affected operators to continue to operate within the bounds of the laws in both States.

6.1.6 Extra Territoriality

Strictly interpreted, extra-territoriality at international law means the attempt of one State to apply its laws outside its territory[26] and there is a general presumption

[26] Shaw (2003) at pp. 611–612.

against the application of extra-territoriality.[27] In the 1979 case of *Mannington Mills* v. *Congoleum Corporation*[28] the United States Supreme Court extended the concept of extra territoriality by introducing a test of balance that ensured consideration by one State for the interests of another State.

The above principle of extra-territoriality might not sit comfortably in the instance of a State requiring PNR data from a flight over-flying its territory as there is no *stricto sensu* application of a requirement in a foreign territory. The most fundamental principle of public international law, that of State sovereignty, is embodied in Article 1 of the Chicago, thus importing the principle into the tenets of air law. This Article provides that Contracting States recognize that every State has complete and exclusive sovereignty over the air space above its territory. The territory of a State, for the purposes of the Convention, cover the land areas and territorial waters adjacent to and under the sovereign, suzerainty, protection and mandate of the State concerned.[29] Arguably, these provisions would give the United States the right *in limine* to prescribe requirements on aircraft flying over its territory. Article 12 of the Chicago Convention provides, *inter alia*, that each contracting State undertakes to adopt measures to insure that every aircraft flying over or manoeuvring within its territory and that every aircraft carrying its nationality mark, wherever that aircraft may be, shall comply with the rules and regulations relating to the flight and manoeuvre of aircraft there in force. This rule can apply to a foreign carrier who is over-flying the territory of any State having a regulation that certain data pertaining to a flight that over-flies its territory has to be submitted to that State. Also important is Article 9 of the Convention, which allows a Contracting State to restrict or prohibit an aircraft from flying over its territory for reasons of military necessity or public safety. The provision goes on to say that each contracting State could also reserve the right, in exceptional circumstances or during a period of emergency, or in the interest of public safety and with immediate effect, temporarily to restrict or prohibit flying over the whole or part of its territory, provided such action would apply without distinction of nationality to aircraft of all States.[30]

At the 28th Session of the International Law Association held in Madrid in 1913, the meeting drew up text which stated that it was the right of every State to enact prohibitions, restrictions and regulations as it may think proper in regard to passage of aircraft through the airspace above its territory and territorial waters.[31] However,

---

[27] *Holmes* v. *Bangladesh Biman Corporation* [1989] 1 AC 1112 at 1126. Also, *Air India* v. *Wiggins* [1980] 1 WLR 815 at 819. In the 1991 case of *EEOC* v. *Arabian American Oil Company and ARAMCO Services* 113 L E 2d 274, the US Supreme Court held that the practice of extra territoriality by one State against the other cannot in any way be justified under the principles of public international law.

[28] 595 F.2d 1287; 66 ILR at 487. See also *Timberlane Lumber Company* v. *Bank of America*, 549 F 2d 597 (1976); 66 ILR at 270.

[29] Chicago Convention, *supra*, Article 2.

[30] *Id.* Article 9 b).

[31] International Law Association, 28th Report, Madrid, 1913, 533–545 at 540.

the text contained a caveat that such restrictions should be subject to the rights of subjacent States and the liberty of passage of aircraft of every nation.[32] The balance advocated at the Madrid meeting of the ILA goes to show that even as early as the beginning of the last century, the thinking was that a State ought to allow other States free passage for their aircraft through the airspace above its territory. There is no doubt that the same position prevails even now, particularly through the currently applicable International Air Services Transit Agreement (IASTA) which was concluded at the same time as the Chicago Convention in December 1944 and has been ratified by many ICAO Contracting States. IASTA allows aircraft of foreign States freedom of peaceful transit (over the airspace of a State) and freedom of making non-traffic (non-revenue) stops for such purposes as refuelling and repair. It has been acknowledged that without these two freedoms, the air transport industry could not survive[33]

The above discussion brings one to the inexorable conclusion that there are two major issues at stake. The first is whether the OPNR is an acceptable tool which helps in enhancing facilitation and security measures in air transport. The answer to this question, as provided by the 12th ICAO Facilitation Division in March/April 2004 and subsequently by the ICAO Council[34] is a resounding "yes". This affirmation brings to bear the need to consider whether the PNR should be used strictly as intended, firstly to facilitate customs and immigration procedures regarding persons and secondly to advise States in advance of persons on board an aircraft approaching their territory for purposes of landing there, enabling States to determine appropriate security clearance measures. The security angle of the PNR brings one to the second issue, as to whether a State can use information contained in the PNR to disallow the right of passage to an aircraft flying over its territory, thereby denying that aircraft a fundamental right acknowledged by States through IASTA.

The second issue raises the question of extra territoriality, which can be answered by invoking Articles 9 and 12 of the Chicago Convention, as earlier discussed. These provisions clearly give a State the right to prohibit an aircraft from over-flying its territory if it believes that such over-flying could be a security hazard. The final issue would be to determine the extent to which a State could exercise its right without touching the sensitivities and dignity of a State in an instance where an aircraft plying domestic services within two points in its territory but passes through the airspace of the prohibiting State is disallowed from using the right of passage.

The entire issue of diversion of an aircraft which is exercising its fundamental right of passage, and the justification of a State for disallowing that aircraft from using that fundamental right hinges on the circumstances prevailing at the time. As was mentioned earlier, this is no legal issue as the question of extra-territoriality does not arise with regard to action taken by a State within its territory. The

[32] Madrid Report, *Id*, at 538.
[33] Honig (1956) at 29.
[34] *Ibid*.

fundamental postulate in the debate is that sovereignty should no longer mean the mere exercise by one State of rights over its territory but should also mean the right of that State to ensure the safety and security of its citizens as well as the integrity of the State.

Public international law is increasingly becoming different from what it was a few decades ago. It can be said with some justification that international law is the thread which runs through the fabric of international politics and provides the latter with its abiding moral and ethical flavour. Without principles and practices of international law, foreign policy would be rendered destitute of its sense of cooperation and become dependent on a nation's self interest. As President Woodrow Wilson once claimed:

> It is a very perilous thing to determine the foreign policy of a nation in the terms of material interests . . . we dare not turn from the principle that morality and not expediency is the thing that must guide us, and that we will never condone equity because it is convenient to do so.[35]

This statement, made in 1950, has great relevance today, when continued progress is being made in technological and economic development and policy decisions of States have far reaching consequences on a trans-boundary basis. Nation States are becoming more interdependent, making decisions made by a particular State in its own interest have a significant negative impact on the interests of other States. Therefore ethics in foreign policy has largely become a construct which combines cultural, psychological and ideological value structures. Within this somewhat complex web of interests, decisions have to be made, which, as recent events in history have shown, require a certain spontaneity from the international community. For example, when Iraq invaded Kuwait in 1990, the members of the United Nations chose economic sanctions against Iraq, claiming that war was the last resort to be embarked upon against Iraq if economic sanctions did not prove to have any effect. In hindsight, one could argue one way or another, firstly, as did the United States, that the use of force bore quick results and, on the hand, as did many officials in Paris, Moscow, Ottawa and Washington, that the decision to wage war against Iraq was too precipitous as not enough time had been given to economic sanctions to compel Iraq to retreat from Kuwait. The precipitous but quick action taken in going to war with Iraq might be justified by some with the analogy of Britain appeasing Hitler in the 1930s without adopting a more aggressive and perhaps belligerent attitude toward German atrocities. This action, which was later labeled as folly by most political scientists, was applauded and endorsed at that time in the British Parliament. In the absence of extra territoriality the only balancing factor in favor of State which orders the diversion of an aircraft overflying its territory, on the basis that persons therein are unacceptable is to have sound justification for doing so in the interests of security and safety.

[35] Quoted in Morganthau and Thompson (1950) at p. 24.

6.1.7 Public Key Directory

Aviation has reached the stage where quantum physics not only assists in the aeronautical aspects of air transport but also contributes to the day to day activities involving passenger clearance, immigration and customs. A brand new technique known as quantum cryptography is on the way, calculated 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. This article examines the technical and legal consequences that might flow from the use of the public key directory.

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.[36] 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

[36] 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*, 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 9303/3* Third Edition 2005, 1-1 to 1-3.

suppliers, and that a technology, once put in place, must be operable or at least retrievable for a period of 10 years.

The Public Key Directory is a central repository for all public keys that are established individually by States. A key is a string of characters which is used to encrypt or decrypt critical information in a document. Therefore the PKI system ensures that digital signatures assigned to data (and not the data itself) in a MRTD are encrypted or decrypted using both a private key—which is used by the passport issuing authority to encrypt the digital signature—and a public key—to be used by the party reading the document to decrypt the signature. Both the private key and the public key play critical roles in the process of encryption and decryption, which is the essence of the public key directory. It is integral to the programme to have an efficient and commonly accepted means of sharing and updating the public keys in effect for all non-expired passports in existence for all participating countries at a given time. Each participating State will therefore install its own secure facilities to generate key pairs. In each case the private key, used to encrypt digital signatures, will be held secret by the State. The public key, on the other hand, can be released for circulation in the public domain. The reading authority at the point of entry would use the appropriate public key to decrypt the information in order to verify whether the data in the MRTD has been altered in any way.

Public key encryption is purely a mathematical process designed to scramble and unscramble messages using two keys (the public key and the private key) and numerical data which contain information the process scrambles the contents of a message. The keys are shared between the scrambler and the un-scrambler. When translated to the e-passport the process works in the following way. The State which issues the passport encrypts information that is placed in the passport using its private key. The State which examines the passport (on arrival of the passenger) obtains the issuing State's public key and uses it to decrypt the information in the passport.

Contrary to popular belief, the PKD is neither a database of e-passports nor a repository of passport information. It is also not a look-out list nor is it a list of persons. Above all, it is not a large database as it remains a database only of public keys. Public keys do not carry personal information but are decoders of information that have been encrypted. The encryption process entitles a reading State to decode the encrypted digital signature on the mandatory passport data which cannot readily be deciphered. Other mandatory data in the machine readable zone of the passport, such as the facial image (photograph) of the passport holder, which is readily visible, do not fall within the process of decryption.

Public keys contain information that can and should be released into the public domain in order to provide for a globally interoperable system that authenticates the contents of integrated circuit chips in passports. There is thus no security issue involved in any potential user's access to public keys, and distribution via the Internet is planned. However, access to the web site will effectively be limited to the users of the system, and specialized system protocols will be required in such transactions. The transmission of key certificates from e-passport issuing States to ICAO, however, will require protection to ensure that bogus keys are not inserted

into the system. One of the requirements to be placed on the successful contractor is to demonstrate the capability and competence to build a system with the necessary security measures. The rules and regulations will require adherence to procedures necessary to implement these measures.

The operation of the PKD and the transactions between the PKD and the users will be relatively simple. The PKD will function as a sort of message board, containing "messages" (public key lists) posted by ICAO after ICAO has verified them as genuine. Contributing administrations will be required to send their key lists to ICAO for posting well in advance of their effective date. Accessing the PKD to verify individual passports is not contemplated. Entities using the system will periodically download the whole directory to update the lists in their own systems and use these lists to verify individual passports. This arrangement, together with the redundancy built into the system, is expected to mitigate the risks associated with any system failure. However, the expected level of system performance will be stipulated in the contract with the PKD operator.

6.1.8 ICAO's Role Regarding the Public Key Directory

In May 2003, the ICAO Council considered work[37] conducted by its Air Transport Committee[38] and the approval by the Committee of a "Blueprint" for incorporating biometric identification in passports and other MRTDs for the purpose of ascertaining and verifying identity. The Committee had taken into consideration a rigorous and sustained 6-year study of technology options for introducing the capability to link a document positively to the rightful holder and to verify the authenticity of the document. The study itself had resulted in a four-part recommendation of the TAG/MRTD. The Blueprint specifies that the primary biometric to be used worldwide will be the face and that the compressed image of the face will be stored, along with the data from the machine readable zone of the passport, in a contact-less Integrated circuit chip. The validity of the data in the chip has to be ensured and, in order to give the reader that assurance, the data in the chip, as well as the facial image, will be digitally "signed". The Committee was apprised that a specially tailored public key infrastructure (PKI) scheme had been specified in order to protect the signed data from counterfeiting or unauthorized alteration by ensuring that any overwriting of data on the chip does not go undetected. The basic

[37] See Establishment of A Public Key Directory (PKD), C-WP/12384, 19/11/04 Revised, 2/2/05, presented to the Council by the Secretary General.

[38] Article 54 d) of the Chicago Convention provides that it shall be a mandatory function of the ICAO Council to appoint and define the duties of an Air Transport Committee, which shall be chosen from among the representatives of the members of the Council and which shall be responsible to it. The Committee is therefore a subordinate body of the Council which largely considers work conducted by the Secretariat in the field of air transport prior to forwarding such work to the Council for final consideration.

premise underlying the study and the recommendation of the TAG/MRTD was that, in the absence of any PKI, the trustworthiness of data in a chip, and hence the global interoperability of the e-passport, cannot be assured.

Based on the above, the TAG-MRTD recommended to the Air Transport Committee that ICAO be the designated Organization to oversee the PKD. This recommendation was based on an interpretation provided to the Council, by the TAG/MRTD, that ICAO had a clear mandate under the Chicago Convention[39] to adopt standards dealing with customs and immigration procedures and to provide for compliance with, *inter alia*, passport laws and regulations, taking into consideration the Organization's sustained and long track record as the developer of MRTD standards, and its international stature as a UN agency. Furthermore, it was claimed that an oversight role in the PKD is deemed particularly appropriate for ICAO due to its substantial interest in document security as an essential component of the aviation security and facilitation programmes elaborated in Annexes 9 and 17. It was the view of the TAG/MRTD that a politically neutral site overseen by ICAO and funded by the e-passport issuing States would provide a trusted resource from which government inspection agencies, airlines, and other entities in all member States might download all public keys in circulation for the purpose of verifying the authenticity of passports as documents of identity, with full confidence that the keys were genuine. It was further contended that, in this regard, an important function of ICAO would be to receive the public keys sent in by issuing States by diplomatic means and perform a technical "due diligence" procedure to verify their authenticity before uploading them to the data base.

The Council was also advised that, in playing an oversight role, ICAO would not be authenticating individual passports or their content. Authentication of a passport remains the function and responsibility of the government agency or aircraft operator examining it.

The envisioned scheme involved the oversight of a central public key directory by ICAO, which was deemed essential for a cooperative, interoperable regime for passport security that will be accessible by all member States. Furthermore, it was contended that a central PKD would be accessible by aircraft operators, who are on the "front lines" as the first to examine the passports of travellers. As a deterrent to the fraudulent alteration or counterfeiting of passports, or the use of stolen passports by imposters to gain access to aircraft, PKI is potentially a most effective anti-terrorism and aviation security measure.

In terms of organizational matters, the proposal for ICAO's oversight role involves two components, *i.e.* maintaining and administering the PKD, both of which would be funded by the fees collected from States issuing e-passports and

[39] Chicago Convention, *Supra*, Articles 13, 23 and 37j. Although Article 37 (j) is directly in point, it is somewhat questionable as to whether Articles 13 and 33 bestow upon ICAO any special mandate to address the need to develop machine readable travel documents and technology related thereto. Article 13 merely states that the laws of States with regard to various aspects of entry and departure should be complied with. Article 23 provides that each Contracting State undertakes, *inter alia*, to establish customs and immigration procedures.

uploading their public keys. As the supervisory authority, ICAO would act on behalf of e-passport issuing States; be responsible for establishment of the PKD system, appointment of the PKD operator; and providing oversight of the system operation, financial matters and policies as decided or approved by the Council. In this regard ICAO's functions would include: receipt of new key certificates from e-passport issuing States, verification of their authenticity, and formal acceptance and uploading to the PKD; liaison with all country contributors and users, and with contractor operational staff, in administrative and operational matters such as new country sign-up and collection of fees; calculation of proposed fee schedules; distribution of revenue to the PKD operator and relevant ICAO units, and development of the regulations and procedures manuals; and periodic reporting to the Council on all of the above matters.

Separately, the contractor chosen or the PKD operator would have the responsibility to design, install and operate the PKD system in accordance with the contractual agreement made with ICAO. The PKD operator would provide data base services not only to contributing States but also to States and other entities using the keys to verify e-passports presented to them.

As for financial management and outlay, the proposal for ICAO involvement in the PKD as outlined above will be based and carried out on the principles of cost-recovery, whereby fees from the States that produce e-passports and send their public keys to ICAO for uploading to the Directory will support administrative and other expenses incurred. At the time of writing, ICAO had already received an advance contribution from one member State and had received letters of intent and requests for invoices from several others. The cost-income formula will be calculated on a schedule of country sign-up fees and annual user fees based on the total estimated cost of a 5-year operation and the number of countries expected to sign up in each year. A special account would be set up in ICAO for the receipt and distribution of contributions and assessments.

Essentially, there will be three main protagonists in the PKD process. Firstly there would be the "group" of e-passport issuing States, comprising a group that would be constituted as a legal body with its own governance structure. This body would be the owner of the PKD and determine independently its mode of operations—including membership, and financial operations. Secondly, there would be ICAO, duly authorized by the Council to act as an agent of the Group, with defined responsibility for providing advice to the Group and executing the work of the group based on agreed terms and conditions. It is envisioned that such an arrangement would cover ICAO against any financial liability arising either from contracting with a third party or a shortfall in the finances of the group. The Group, as a whole, should underwrite the financing of the activities undertaken by ICAO. The last person in the triangle is the contractor, who is appointed either by the group or by ICAO on authority granted by the Group. ICAO's responsibility for the management of the contractor's activity would be defined by the Group.

6.1.9 Legal Liability of ICAO

As stated above, ICAO's responsibility with regard to oversight of the PKD process would involve two areas, i.e. maintenance and administration. A host of functions are attached to these two supervisory functions, such as acting on behalf of e-passport issuing States, and being responsible for establishment of the PKD system, appointment of the PKD operator and providing oversight of the system operation, financial matters and policies as decided or approved by the Council. The first question that arises in regard to ICAO's legal status is whether the Organization has the legal capacity to perform the abovementioned functions and be responsible for them. In other words, if ICAO's legal liability were to be questioned in a court of law in any jurisdiction of an ICAO member State, would the courts recognize ICAO as having the legal capacity to assume these functions and be legally accountable for them?

6.2 Security of Aircraft and Passengers

Aviation is an important global business and a significant driver of the global economy. It is vital, therefore, that stringent measures are taken to counter acts of unlawful interference with civil aviation. The *Convention on International Civil Aviation* signed at Chicago on 7 December 1944, states in its *Preamble* that whereas the development of civil aviation may help preserve friendship and understanding among the people of the world, yet, its abuse could become a threat to general security.

The genealogy of the term "*Terrorism*" lies in Latin terminology meaning "to cause to tremble" (*terrere*). Since the catastrophic events of 11 September 2012, we have seen stringent legal measures taken by the United States to attack terrorism, not just curb it. The famous phrase "war on terror" denotes pre-emptive and preventive strikes carried out through applicable provisions of legitimately adopted provisions of legislation. The earliest example is the *Air Transportation Safety and System Stabilization Act* (ATSAA) enacted by President Bush less than 2 months after the 9/11 attacks. Then, 2 months after the attacks, in November 2001, Congress passed the *Aviation and Transportation Security Act* (ATSA) with a view to improving security and closing the security loopholes which existed on that fateful day in September 2001. The legislation paved the way for a huge federal body called the Transportation Security Administration (TSA) which was established within the Department of Transportation. The Homeland Security Act of 2002 which followed effected a significant reorganization of the Federal Government.

Since the events of 11 September 2001, there have been several attempts against the security of aircraft in flight. These threats have ranged from shoe bombs to dirty bombs to explosives that can be assembled in flight with liquids, aerosols and gels.

In every instance the global community has reacted with pre emptive and preventive measures which prohibit any material on board which might seemingly endanger the safety of flight. Some jurisdictions have even gone to extremes in prohibiting human breast milk and prescriptive medications on board.

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 dangerous pathogens on board, the use of cyber technology calculated to interfere with air navigation systems, and the misuse of man portable air defence systems are real and have to be addressed with vigour and regularity. ICAO has been addressing these threats for some time and continues to do so on a global basis.

It is a platitude to say that aviation security is a largely reactive process. It will be recalled that after the spate of hijackings in the late 1960s and 1970s, States rushed to install detectors with X-Ray capability at the entrance to the aircraft gate. Then, as the *displacement theory*[40] demonstrated, terrorists moved their attention towards attacking airports, which prompted States to install screening equipment at centralized points in the terminal itself. In similar vein, in the aftermath of the attempted bombing of an aircraft on 25 December 2009 by a person who is alleged to have carried explosives in his undergarments, some States began to look seriously into tightening airport security, particularly through a more stringent body scanning process. While the United States toughened screening measures on US bound flights, particularly with regard to passengers arriving from 14 targeted nations,[41] airports in the United Kingdom began the use of full body scanners at both Heathrow and Manchester airports.[42] In Canada, Rob Merrifield, Minister of State for Transport is reported to have stated that 44 scanners have been ordered to be used on passengers selected for secondary screening at Canadian airports. The machines, which can scan through clothing, will be installed in Vancouver, Calgary, Edmonton, Winnipeg, Toronto, Ottawa, Montreal and Halifax.[43] This measure is partly due to the fact that the Christmas day incident was later classified as having occurred due to a serious lapse in security.

[40] The Displacement Theory suggests that removing opportunity for crime or seeking to prevent a crime by changing the situation in which it occurs (see Situational Crime Prevention) does not actually prevent crime but merely moves it around. There are five main ways in which this theory suggests crime is moved around: crime can be moved from one location to another (geographical displacement); crime can be moved from one time to another (temporal displacement); crime can be directed away from one target to another (target displacement); one method of committing crime can be substituted for another (tactical displacement); and one kind of crime can be substituted for another (crime type displacement).

[41] Afghanistan, Algeria, Cuba, Iran, Iraq, Lebanon, Libya, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen. See US Toughens Screening for US-Bound Flights, *Air Letter*, No. 16896, Monday 04 January 2010, at 1.

[42] UK Airports Commence Use of Full Body Scanners, *Air Letter*, No. 16918, Wednesday 03 February 2010 at 2. According to this report, scanning equipment were scheduled to be installed in Birmingham in late February 2010. *Ibid.*

[43] CBC News, January 5, 2010. See: http://www.cbc.ca/canada/story/2010/01/05/security-canada-us-airport.html#ixzz0eVT3wBNY.

In response to the attempted sabotage of Northwest Airlines Flight 253 on 25 December 2009,[44] ICAO used the AVSEC Point of Contact (PoC) Network to communicate information and recommendations to participating States, numbering 99 as of 31 May 2010. States were encouraged to conduct risk assessments and implement appropriate screening measures in light of the incident, and were reminded of the need for cooperation in all matters related to aviation security. The 21st meeting of the AVSEC Panel was held at ICAO Headquarters from 22 to 26 March 2010. The Panel considered the threat and risk environment in light of the attempted sabotage of 25 December 2009 and issued a number of recommendations. Provisions in Annex 17 to the Chicago Convention on Security were updated and strengthened, and are expected to become applicable in 2011, following formal consultation with Member States and approval by the Council.

6.2.1 Body Scanners

Full body scanners, costing about $250,000 each and claimed by some security experts as an effective tool in detecting hidden explosives, show the contours of the human body as well as body parts in some detail, prompting some to question the legality and ethical justification of their use. In the United States, passengers handpicked for a full-body scan can opt out of the screening, but if they do, they must submit to full-body pat-downs by an officer of the Transport Security Administration (TSA).[45] The technology was introduced a couple of years ago, but U.S. airports have been slow to install the machines, partly because of privacy concerns raised by some members of Congress and civil liberties groups.

It must be noted that in the United States, the Fourth Amendments states:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[46]

The significance of this provision lies in the fact that the prohibition is against unreasonable searches, and that too by agents of the governments, the latter fact being borne out by a strong *cursus curiae* in the United States.[47] It can therefore be assumed that the Fourth Amendment may not be applicable in instances where scanning is carried out by airport security officers who are not government agents.[48] If, however, the scanning at the airport is conducted by officers of the government,

[44] For a discussion of this incident, See Abeyratne (2010), pp. 167–181.

[45] Rucker (2010) at 1.

[46] *US Constitution*, Article 1 Sec. 4 Clause 6.

[47] See Sweet (2008) at 45.

[48] *Ibid*.

by law, the consent of the passenger has to be obtained before such scanning is carried out.[49]

States which are installing full body scanners are fully aware that their use could bring to bear issues of privacy. However, it should be noted that this is just one more reactive step—to ensure that no person enters an aircraft with explosives hidden in his underwear—and the only known way to respond to this new threat is to use full body scanner. The question then arises as to whether the responsibility of the State toward its constituents and those using aircraft for transport from and to their territory, to prevent private acts of terrorism overrides the right of privacy of the individual. This article will address the balance between the two interests.

6.2.2 Privacy Rights of the Person

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".[50]

The Chicago Convention embodies in its *Preamble* the need to create and preserve friendship and understanding among the nations and peoples of the world, and cautions Contracting States that the abuse of this friendship and understanding can become a threat to general security. 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:

---

[49] See *US* v. *Favela* 247 F.3d.838, 2001 and *U.S*. v. *Eustaquio* 198 R.3d 1068 (8th Cir.1999).

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

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.[51]

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.[52] The subject of privacy has been identified as an intriguing and emotive one.[53] 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.[54] 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.[55] 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.[56]

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.[57] 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,

[51] Hoffman (1980), p. 142.

[52] Abeyratne (2001), pp. 153–162. Abeyratne (2002b), pp. 83–115.

[53] Young (1978) at 1.

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

[55] 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 20 page dossier on every man, woman, and child in the world. See Jones (1973).

[56] Westin (1970) at 124.

[57] Orwell (1978).

including, food inclination, leisure activities, and consumer credit behaviour.[58] 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.[59] 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".[60]

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*.[61] Thereafter, several other human rights conventions followed the same trend, granting to individuals the fundamental right of privacy.[62] The pre-eminent concern of these international instruments was

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

[59] 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.

[60] 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.

[61] 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.

[62] 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.

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.[63] 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,[64] and culminating in the control over one's personal information.[65] 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,[66] in 1890.[67] 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,[68] 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.[69] 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.[70]

---

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

[64] 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.

[65] 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), pp. 447–448. See also Hoffer (2000) at 8.1.; Gavison (1980), p. 421.

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

[67] The definition of privacy as the "Right to be Alone" is often erroneously attributed to Warren and Brandeis. See Warren and Brandeis (1980). 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*].

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

[69] See Reidenberg (1995) at 498.

[70] 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. 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*.[71]

It must be borne in mind that privacy is not an absolute, unlimited right that operates and applies in isolation.[72] 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.[73] 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[74] (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.[75]

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.

As for the use of information resulting in a full body scan, such information is purely biological and should be used only for purposes of identifying weapons or dangerous objects on the person with an explicit undertaking by the authorities concerned who use the information that it will not be used for any purpose other

---

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

[72] See Simmel (1971) at 71.

[73] 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 Montgomery Curtis (1992) at 2.

[74] Hoffman (1980) at 146.

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

than for purposes of scanning. Before a process for the collection of such information is formally put into practice, legal issues pertaining to privacy, cultural sensitivity and ethical justification should be carefully thought out, and given foremost consideration.

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).[76]

In the body scanning process, there is an implicit link between ownership rights and privacy. Data protection legislation, including data privacy laws have been enacted by many countries throughout the world for two main reasons: protection of privacy; and ensuring of access by the owner to his information stored in a computer. Although the exact nature can vary from State to State, there is a common thread that weaves itself into the fabric of legislation in general, to ensure that: data is obtained by lawful means and processed in a fair manner; data is stored for the legitimate purpose intended and not used for any purpose incompatible with the original purpose; the collection of data is done in a reasonable manner and not excessively in order to store data over and above what is necessary; the accuracy of the data should be ensured; and the time of preservation of data is limited to the period during which such data is used.

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.

6.2.3 Security of the State

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

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

would be the security of State. Inherent to the concept of security of State is State responsibility 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.[77]

At the core of the principal–agent dilemma is the theory of complicity, which attributes liability to a State that was complicit in a private act. Hugo Grotius (1583–1645), founder of the modern natural law theory, first formulated this theory based on State responsibility that was not absolute. Grotius' theory was that although a State did not have absolute responsibility for a private offence, it could be considered complicit through the notion of *patienta* or *receptus*.[78] While the concept of *patienta* refers to a State's inability to prevent a wrongdoing, *receptus* pertains to the refusal to punish the offender.

The eighteenth century philosopher Emerich de Vattel was of similar view as Grotius, holding that responsibility could only be attributed to the State if a sovereign refuses to repair the evil done by its subjects or punish an offender or deliver him to justice whether by subjecting him to local justice or by extraditing him.[79] This view was to be followed and extended by the British jurist Blackstone a few years later who went on to say that a sovereign who failed to punish an offender could be considered as abetting the offence or of being an accomplice.[80]

A different view was put forward in an instance of adjudication involving a seminal instance where the Theory of Complicity and the responsibility of states for private acts of violence was tested in 1925. The case[81] involved the Mexico–United States General Claims Commission which considered the claim of the United States on behalf of the family of a United States national who was killed in a Mexican mining company where the deceased was working. The United States argued that the Mexican authorities had failed to exercise due care and diligence in apprehending and prosecuting the offender. The decision handed down by the Commission distinguished between complicity and the responsibility to punish and the Commission was of the view that Mexico could not be considered an accomplice in this case.

---

[77] Caron (1998) at 153–154 cited in Becker (2006a) at 155.

[78] Grotius and Scott (1646), pp. 523–526.

[79] De Vattel and Fenwick (1916), p. 72.

[80] Blackstone and Morrison (2001) at 68.

[81] *Laura M.B. Janes* (*USA*) v. *United Mexican States* (1925) 4 R Intl Arb Awards 82.

The Complicity Theory, particularly from a Vattellian and Blackstonian point of view is merely assumptive unless put to the test through a judicial process of extradition. In this Context it becomes relevant to address the issue through a discussion of the remedy.

The emergence of the Condonation Theory was almost concurrent with the *Jane* case[82] decided in 1925 which emerged through the opinions of scholars who belonged to a school of thought that believed that States became responsible for private acts of violence not through complicity as such but more so because their refusal or failure to bring offenders to justice, which was tantamount to ratification of the acts in question or their condonation.[83] The theory was based on the fact that it is not illogical or arbitrary to suggest that a State must be held liable for its failure to take appropriate steps to punish persons who cause injury or harm to others for the reason that such States can be considered guilty of condoning the criminal acts and therefore become responsible for them.[84] Another reason attributed by scholars in support of the theory is that during that time, arbitral tribunals were ordering States to award pecuniary damages to claimants harmed by private offenders, on the basis that the States were being considered responsible for the offences.[85]

The responsibility of governments in acting against offences committed by private individuals may sometimes involve condonation or ineptitude in taking effective action against terrorist acts, in particular with regard to the financing of terrorist acts. The United Nations General Assembly, on 9 December 1999, adopted the International Convention for the Suppression of the Financing of Terrorism,[86] aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. One of the treaties cited by the Convention is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.[87]

The Convention for the Suppression of the Financing of Terrorism also provides that, over and above the acts mentioned, providing or collecting funds toward any

[82] *Ibid.*

[83] *Black's Law Dictionary* defines condonation as "pardon of offense, voluntary overlooking implied forgiveness by treating offender as if offense had not been committed."

[84] Jane's case, *Supra* note 82, at 92.

[85] Hyde (1928) at 140–142.

[86] International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.

[87] A/52/653, 25 November 1997.

other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

The United Nations has given effect to this principle in 1970 when it proclaimed that:

> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[88]

Here, the words *encouraging* and *acquiescing in organized activities within its territory directed towards the commission of such acts* have a direct bearing on the concept of condonation and would call for a discussion about how States could overtly or covertly encourage the commission of such acts. One commentator[89] identifies three categories of such support: *Category I* support entails protection, logistics, training, intelligence, or equipment provided terrorists as a part of national policy or strategy; *Category II* support is not backing terrorism as an element of national policy but is the toleration of it; *Category III* support provides some terrorists a hospitable environment, growing from the presence of legal protections on privacy and freedom of movement, limits on internal surveillance and security organizations, well-developed infrastructure, and émigré communities.

Another commentator[90] discusses what he calls the *separate delict theory'* in State responsibility, whereby the only direct responsibility of the State is when it is responsible for its own wrongful conduct in the context of private acts, and not for the private acts themselves. He also contends that indirect State responsibility is occasioned by the State's own wrongdoing in reference to the private terrorist conduct. The State is not held responsible for the act of terrorism itself, but rather for its failure to prevent and/or punish such acts, or for its active support for or acquiescence in terrorism.[91] Arguably the most provocative and plausible feature in this approach is the introduction by the commentator of the desirability of determining State liability on the theory of causation. He emphasizes that:

> The principal benefit of the causality based approach is that it avoids the automatic rejection of direct State responsibility merely because of the absence of an agency relationship. As a

[88] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, UN General Assembly Resolution 2625 (XXV) 24 October 1970.

[89] Steven Metz, State Support for Terrorism, Defeating Terrorism, Strategic Issue Analysis, at http://www.911investigations.net/IMG/pdf/doc-140.pdf.

[90] Becker (2006b).

[91] *Id.* Chapter 2, 67.

> result, it potentially exposes the wrongdoing State to a greater range and intensity of remedies, as well as a higher degree of international attention and opprobrium for its contribution to the private terrorist activity.[92]

The causality principle is tied in with the rules of State Responsibility enunciated by the International Law Commission and Article 51 of the United Nations Charter which states that nothing in the Charter will impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. The provision goes on to say that measures taken by Members in the exercise of this right of self-defense will be immediately reported to the Security Council and will not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

The conclusion to this discussion is inevitable, *i.e.* security of the State is paramount and the State can legislate to ensure that measures are taken to guarantee that security. However, as the case law cited in this article reflects, these measures have to conform to the constitutional guarantees given to citizens, one of which is the Fourth Amendment to the United States Constitution. In this context, the consent of the individual selected for a full body screen is essential and a full body scan taken by the State or an instrumentality of that State without a person's consent would tantamount to a breach of the Fourth Amendment. In the final analysis, however, the State is answerable to the public to show that it took every measure to avoid clear and present danger. The responsibility of a State for private acts of individuals which unlawfully interfere with civil aviation is determined by the quantum of proof available that could establish intent or negligence of the State, which in turn would establish complicity or condonation on the part of the State concerned. One way to determine complicity or condonation is to establish the extent to which the State adhered to the obligation imposed upon it by international law and whether it breached its duty to others. In order to exculpate itself, the State concerned will have to demonstrate that either it did not tolerate the offence (by using such measures as body scanners) or that it ensured the punishment of the offender. *Brownlie* is of the view that proof of such breach would lie in the causal connection between the private offender and the State.[93] In this context, the act or omission on the part of a State is a critical determinant particularly if there is no specific intent.[94] Generally, it is not the intent of the offender that is the determinant but the failure of a State to perform its legal duty in either preventing

[92] Becker (2006b) at 335.

[93] Brownlie (1983) at 39.

[94] Report of the International Law Commission to the United Nations General Assembly, UNGOAR 56th Session, Supp. No. 10, *UN DOC A/56/10*, 2001 at 73.

the offence (if such was within the purview of the State) or in taking necessary action with regard to punitive action or redress.[95]

A perceived inadequacy of the global framework of aviation security is the lack of an implementation arm. ICAO has taken extensive measures to introduce relevant international conventions as well as Standards and Recommended Practices (SARPs) in Annex 17 to the Chicago Convention. There is also a highly classified *Aviation Security Manual* developed by ICAO which is provided to States. Additionally, the Organization provides focused security training courses to its member States. However, ICAO's role is largely confined to rule making and the provision of guidance, bringing to bear the need for an aviation security crisis management team on a global scale that could work towards effectively precluding acts of terrorism.

Another measure that could proactively facilitate the arrest of terrorism is the global curbing of the financing of terrorism. The United Nations General Assembly, on 9 December 1999, adopted the International Convention for the Suppression of the Financing of Terrorism, aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. The treaties listed are those that are already adopted and in force and which address acts of unlawful interference with such activities as deal with air transport and maritime transport. Also cited is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

The *Convention for the Suppression of the Financing of Terrorism* also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

The above notwithstanding, one cannot ignore the incontrovertible fact that security is a systemic process. The mere use of full body scanners by no means ensures total security against acts of unlawful interference with civil aviation. As the Christmas day incident showed, intelligence gathering, sharing of information, and more importantly, integration and analysis of such information[96] are critical to

[95] de Arechaga (1968) at 535.

[96] As stated by President Obama, "this was not a failure to collect intelligence. . .it was a failure to integrate and understand the intelligence that we already had. . ." Airline Bomber could Have Been Stopped, *The Air Letter*, Tuesday 05 January 2010, No. 16897, at 1.

the security chain. What is most important is to establish a global security culture that ensures the cooperation of the 190 ICAO member States by working in harmony. A perceived inadequacy of the global framework of aviation security is the lack of an implementation arm. ICAO has taken extensive measures to introduce relevant international conventions as well as Standards and Recommended Practices (SARPs) in Annex 17 to the Chicago Convention. There is also a highly classified *Aviation Security Manual* developed by ICAO which is provided to States. Additionally, the Organization provides focused security training courses to its member States. However, ICAO's role is largely confined to rule making and the provision of guidance, bringing to bear the need for an aviation security crisis management team on a global scale that could work towards effectively precluding acts of terrorism.

6.3 Cargo Security and Handling

Many aviation disasters, including the PANAM disaster over Lockerbie, Scotland in 1988 and the Air India disaster off the coast of Ireland in 1985 have been due to explosives packed in cargo containers. Such acts are committed within the premises of the aerodrome. The 37th Session of the ICAO Assembly in 2010 adopted a Declaration unanimously adopted by participants, which reaffirmed international commitment to enhance aviation security collaboratively and proactively through screening technologies to detect prohibited articles, strengthening international standards, improving security information-sharing and providing capacity-building assistance to States in need. The Assembly also put its full support behind a comprehensive, new ICAO aviation security strategy.

At a high level Conference held in ICAO from 12 to 14 September 2012 on aviation security the conference recognized that air cargo advanced information for security risk assessment is a developing area that enhances air cargo security, particularly in the context of express delivery carriers such as FEDEX, UPS, DHL Express and TNT Express who carry around 30 million shipments daily, which typically contain high-value added, time-sensitive cargo. These carriers guarantee the timely delivery of these vast volumes of shipments, ranging from same-day delivery to 72 h after pick-up, virtually anywhere in the world. They operate in 220 countries and territories.

The conference noted that a real risk in the area of cargo and mail security would arise when an express delivery carrier experiences a technical problem in an aircraft and is forced to transfer cargo to a passenger carrier, in which instance strict supply chain standards should be adhered so that the risk in the transfer of cargo could be obviated.

Participants agreed that it was essential that solid standards and mutual recognition programmes be in place in order to make sure that States all along an air cargo supply chain satisfy themselves that air cargo is secure, and so let it flow unimpeded. Such standards and recommended practices should allow for the

speedy transit and transhipment of legitimate air cargo worldwide, through any combination of air routes and transit or transhipment points.

One of the threats to aerodrome security is what is known as the "insider threat" where informants from within the aerodrome (in many instances who are working as staff) alert their accomplices outside with critical security information. In February, a security breach in Antwerp, Belgium led to one of the biggest diamond heists in recent history. Under the cover of darkness, eight gunmen in hooded police clothing gained access through an airport perimeter fence and drove onto the tarmac in two black vehicles with flashing blue police lights. With great speed and precision, the heavily armed thieves sorted through and removed packages from the cargo hold of a parked Helvetic Airways aircraft, loaded them in their vehicles and made a high speed getaway.

Preliminary speculation is that the thieves had inside information or assistance, much like the infamous Lufthansa Heist of 1978 at John F. Kennedy Airport in New York. Aided by the knowledge of an airport employee, members of the Lucchese crime family were able to steal in excess of 6 million dollars in untraceable U.S. currency and jewels from a temporary holding vault on the airport property. Insider knowledge and assistance was central to that crime's success. Ajay Jain, in an article published in January 2013 states:

> Various airline employees, vendors and multiple tenants need to be authenticated every day. Their physical access rights need to be controlled and managed dynamically based upon their role and policies affecting their access. In fact, airports present one of the most complicated scenarios when administering restricted-area access control, identity verification and issuance of an access credential. Many airports have siloed systems and processes used to manage employees' access credentials.
>
> Physical identity and access management operations are handled manually, leading to potentially dangerous errors, a higher cost of operations, enrollment and termination delays and a lower level of security. A multi-layer balance between security, costs and practicality is required to address this issue. Leveraging technologies to achieve security goals can also improve efficiencies and customer service.[97]

Jain states that physical identity and access management software can solve these and related problems by unifying identity management airport-wide, integrating physical security systems, automating processes and simplifying control of employees, vendors and other identities. He states further that software allows airports to manage the lifecycle of identities as they relate to physical access, including synchronized on/off-boarding across all systems harboring an identity record, access profile, zone management and role-based physical access. Comprehensive background check of all personnel selected for hire/employment at an airport needs to be carried out by the relevant State's security agencies based on risk assessment. In addition, re-vetting of airport workers such as cleaners, duty free

[97] Ajay Jain, *Addressing the Insider Threat*, at http://security-today.com/Articles/2013/01/01/Addressing-The-Insider-Threat.aspx.

shop personnel, catering staff and concessionaires must be carried out frequently in order to mitigate collusion to commit acts of unlawful interference.[98]

What has been suggested by experts is a 100 % screening process for all aerodrome employees. One study states:

> Ground crews are largely unseen by the general public. But in much the same way as flight crews, they have intimate knowledge about their work environment. They also have unrestricted access to the exterior and interior of aircraft. Despite this access, these employees are not subject to the same security screenings as passengers and most flight crews.
>
> Ground-crew employees usually access the inner workings of the airport through an employee entrance. This entrance should have a guard present and is accessed by a key, coded lock, biometric device, or other door-locking mechanism. It is not considered a screening checkpoint because its only purpose is to restrict access to unauthorized personnel—not to inspect employees or their belongings. Once inside, however, these individuals are given largely unfettered access to the airport property. They, like flight crews, know the inner workings of the airport and its security weaknesses.[99]

Britain has a programme which vets applicants for sensitive 'airside' jobs to see if they have committed offences abroad. However, those who already hold security passes—including pilots and baggage-handlers—will not be checked. Be that as it may, to effectively respond to insider threat at airports requires predictive risk analytics and utilization of cutting-edge security convergence technology.

6.3.1 Human Remains

Although the carriage of human remains comes within the purview and responsibility of the airline, the aerodrome is the place of loading and adequate facilities have to b provided with sensitivity and understanding. If a person dies in a country other than his own, there are no global rules or guidance that dictates the manner in which his remains could be transported back to his country, with dignity and care. This matter was highlighted in 2003 before the European Parliament with a real example of a British national who died while on holiday in Greece. The Greek authorities had carried out an autopsy which concluded that the deceased tourist had died of a heart attack. When the body was transported back home the deceased's family had requested a second autopsy, only to find that most of the deceased's organs had been removed in Greece after the autopsy and destroyed, according to Greek law. This had caused severe mental distress to the deceased's kin.

The inevitable fact is that there are two dimensions to this subject: the health and sanitation aspects of carrying human remains by air; and the rights of close relatives of the deceased to bring his remains back home with speedy dispatch. It also

[98] The Reality of Mitigating the Insider Threat, *ATCM—WP/11*, 12th Meeting of the AFCAC Air Transport Committee Dakar, Senegal, 30–31 October 2012, at 1.

[99] Goff (2013).

highlights the serious lacuna in regulatory consistency in the carriage by air of human remains and traces attempts by the international community to address the subject. The discussions lead to the conclusion that, although several attempts have been made at international level in the past—some clear and some unclear—they lack unification and stand fragmented and ambivalent. To their credit, airlines, under the guidance of the International Air Transport Association (IATA), have adopted their own principles in carrying human remains with compassion and dedication. The conclusion suggests a way forward in binding the threads of this issue in a harmonious manner.

Human dignity is an international concept which is extended both to the living and the dead. The 1948 *Universal Declaration of Human Rights* of the United Nations—the cornerstone of human dignity—declares that the inherent dignity and the equal and inalienable rights of all members of the human family are the foundations of freedom, justice and peace in the world and that all human beings are born free and equal in dignity and rights. This statement establishes human dignity as the conceptual basis for human rights. Seventy-five percent of the constitutions of ICAO's 191 member States use the concepts of "human dignity" or "personal dignity" explicitly.[100] It follows therefore that if the remains of a human being are not given equal respect and dignity, the moral imperative of the doctrine of human dignity[101] would be rendered destitute of meaning and purpose.

From an aviation perspective, most airlines in the world offer services for the transportation of human remains and cremated remains. These services are varied according to the policies of each airline, but all share a common thread of dedication and compassion in offering the service in the transportation of funeral shipments. Usually, airlines employ specially trained staff to address all the travel-related issues that may arise when shipping such very sensitive cargo. The tasks assigned to these staff include providing advice to those seeking the airlines' services on applicable regulations, taking into account the delicateness of the responsibility that devolves upon the carrier.

In terms of property rights pertaining to a cadaver or other remains, such rights do not exist at common law. However, for the purpose of transportation—whether it be for embalming, cremation or internment—the corpse or cremated remains of a human being is considered to be property or quasi-property, the rights to which are held by the surviving spouse or next of kin. This right cannot be transferred and does not exist while the deceased is living. A corpse or urn carrying cremated remains may not be retained by either an undertaker or a carrier as security for unpaid funeral expenses, particularly if such were kept without authorization and payment was demanded as a condition precedent to its release. Upon burial the

[100] http://www.constitution.org; http://www.oefre.unibe.ch/law/icl; http://www.psr.keele.ac.uk.

[101] Human dignity has not been comprehensively defined and has remained a somewhat squishy subject, often explained theologically. However, the dictionary definition of dignity is that it is *inter alia* "the quality or state of being worthy of esteem or respect". See http://www.thefreedictionary.com/dignity.

body accrues to the ground and any appurtenant property such as jewelry which was on the corpse on burial accrue to their rightful owner as determined by applicable principles of property laws and wills and testaments as they might exist.

The purpose of this article is to discuss *de legelata* the fragmented regime applicable to the carriage by air of human remains. Two antiquated multilateral agreements, one Resolution and one Regulation all in Europe; some maundering by the ICAO Council decades ago; two Annexes to the Chicago Convention which may have applicability to this subject; some proactive guidelines by the International Air Transport Association and the World Health Organization and procedures and policy of individual air carriers comprise the history of this subject. Against this backdrop, this article will inquire into the need for a global regulatory process that would properly address this esoteric but important area of carriage by air.

6.3.2 International Agreements

The Berlin Agreement of 1937

The *International Arrangement Concerning the Conveyance of Corpses*[102] (Berlin Agreement), signed at Berlin on 10 February 1937 was the first recorded attempt at the unification of rules relating to the carriage of human remains. The agreement, which applied to the international transport of corpses immediately after decease or exhumation, was designed to avoid the difficulties resulting from differences in the regulations concerning the conveyance of corpses, and recognized the necessity and the convenience of laying down uniform regulations in this area of transportation. Accordingly, the signatory States[103] undertook to accept the entry into their territory, or the passage in transit through their territory, of the corpses of persons deceased in the territory of any one of the other contracting countries upon certain conditions, which were incorporated in the Agreement.

The initial condition, as laid out in Article 1 of the Agreement was that, for the conveyance of any corpse by any means and under any conditions, a special laissez-passer be issued for a corpse which would state the surname, first name and age of the deceased person, and the place, date and cause of decease. The competent authority for the place of decease or the place of burial in the case of corpses exhumed had to issue the laissez-passer and it was recommended that the laissez-passer should be made out, not only in the language of the country issuing it, but also in at least one of the languages most frequently used in international relations.

[102] League of Nations, Treaty Series 1938, No. 439r at 315–325.

[103] Germany, Belgium, Chile Denmark, Egypt, France, Italy, the Netherlands, Switzerland, Czechoslovakia and Turkey.

The Berlin Agreement further stated that neither the country of destination nor the countries of transit shall require, over and above such papers as are required under international conventions for the purpose of transports in general, any document other than the laissez-passer referred to in Article 1. The following had to be presented to the competent authority for the issuance of laissez-passer: a certified true copy of the death certificate; and official certificates to the effect that conveyance of the corpse is not open to objection from the point of view of health or from the medico-legal point of view, and evidence that the corpse has been placed in a coffin in accordance with the regulations laid down in the Agreement.[104]

As for packaging the human remains, the Agreement, in Article 3 provided that corpses must be placed in a metal coffin, the bottom of which has been covered with a layer approximately 5 cm. of absorbent matter such as peat, sawdust, powdered charcoal or the like with the addition of an antiseptic substance. Where the cause of decease was a contagious disease, the corpse itself was required to be wrapped in a shroud soaked in an antiseptic solution. A further requirement was that the metal coffin must thereupon be hermetically closed (soldered) and fitted into a wooden coffin in such a manner as to preclude movement. The wooden coffin was required to be of a thickness of not less than 3 cm. and its joints must be completely watertight. It was also required that the coffin be closed by means of screws not more than 20 cm. distant from one another, and strengthened by metal hoops. In the case of transport by air, The Agreement, in Article 7, required that coffins must be conveyed either in an aircraft specially and solely used for the purpose or in a special compartment solely reserved for the purpose in an ordinary aircraft.

The Agreement precluded bodies of persons who had died as a cause of plague, cholera, small-pox or typhus from being conveyed between the territories of the contracting parties until the lapse of at least 1 year after the demise. No articles were permitted to be transported along with the coffin in the same aircraft or in the same compartment, other than wreaths, bunches of flowers and the like.[105]

Agreement on the Transfer of Corpses (Strasbourg—1973)

The second international agreement was in 1973 called the *Agreement on the Transfer of Corpses*, and it was drawn up within the Council of Europe by the European Public Health Committee. The Strasbourg Agreement was opened for signature by the member States of the Council of Europe on 26 October 1973. This agreement was designed to adapt the provisions of the Berlin Agreement concerning the conveyance of corpses, to the new situation arising from developments in the field of communications systems, international relations and commercial and tourist activities. A proposal to examine anew the problem of the transfer of corpses with a view to drawing up a new instrument was approved by the

[104] Berlin Agreement, *supra* note 102, Article 2.

[105] *Id.* Article 4.

Committee of Ministers of the Council of Europe in 1967 and this task was entrusted to the European Public Health Committee which, in the course of its work, gave due consideration to the observations, among others, of the European Federation of Funeral Directors (Brussels) and the European Funeral Directors Association (Vienna). The text of the draft Agreement was submitted to the European Committee on Legal Co-operation (CCJ) before its final adoption by the Committee of Ministers of the Council of Europe in April 1973. It was opened for signature by member States of the Council of Europe on 26 October 1973.

The Strasbourg Agreement defines the transfer of corpses as the international transport of human remains from the State of departure to the State of destination. Accordingly, the State of departure is that in which the transfer began; in the case of exhumed remains, it is that in which burial had taken place; the State of destination is that in which the corpse is to be buried or cremated after the transport. The Agreement does not apply to the international transport of ashes. Article 3 of the Agreement states that during the transfer, any corpse is required to be accompanied by a special document (laissez-passer for a corpse) issued by the competent authority of the State of departure. The laissez-passer has to include at least the information set out in the model annexed to the Agreement; and be made out in the official language or one of the official languages of the State in which it was issued and in one of the official languages of the Council of Europe.

Article 4 provides that, with the exception of the documents required under international conventions and agreements relating to transport in general, or future conventions or arrangements on the transfer of corpses, neither the State of destination nor the transit State shall require any documents other than the laissez-passer for a corpse. The laissez-passer is issued by the competent authority referred to in Article 8 of the Agreement,[106] after it has been ascertained that: all the medical, health, administrative and legal requirements of the regulations in force in the State of departure relating to the transfer of corpses and, where appropriate, burial and exhumation have been complied with; the remains have been placed in a coffin which complies with the requirements laid down in Articles 6 and 7 of the Agreement; and that the coffin only contains the remains of the person named in the laissez-passer and such personal effects as are to be buried or cremated with the corpse.

Article 6 requires that the coffin must be impervious and that the inside must contain absorbent material. If the competent authority of the State of departure consider it necessary the coffin must be provided with a purifying device to balance the internal and external pressures. It may consist of: either an outer coffin in wood with sides at least 20 mm thick and an inner coffin of zinc carefully soldered or of any other material which is self-destroying; or a single coffin in wood with sides at least 30 mm thick lined with a sheet of zinc or of any other material which is self-

[106] Article 8 states that each Contracting Party shall communicate to the Secretary General of the Council of Europe the designation of the competent authority referred to in Article 3, paragraph 1, Article 5 and Article 6, paragraphs 1 and 3 of the Agreement.

destroying. If the cause of death is a contagious disease, the body itself is required to be wrapped in a shroud impregnated with an antiseptic solution.

Article 6 further provides that the coffin, if it is to be transferred by air, has to be provided with a purifying device or, failing this, present such guarantees of resistance as are recognised to be adequate by the competent authority of the State of departure. If the coffin is to be transported like an ordinary consignment, it has to be packaged so that it no longer resembles a coffin, and it shall be indicated that it be handled with care.[107]

Resolution 2003/2032 (INI)

The European Community was dissatisfied with both the Berlin Agreement and the Strasbourg Agreement (which only some member States had signed), claiming that these Agreements advocated indirect discrimination by providing for non-European Community residents. Also it was claimed that these two agreements imposed strict rules on the cross-border transfer of mortal remains, applied essentially to 'non-nationals' and hence ran counter to the Community scheme of things. Accordingly, and with a view to addressing the case where a Community citizen expired in a Community country other than his own and his remains had to be repatriated to his country, a Committee was appointed by the European Parliament to consider an instrument that addressed the conveyance of mortal remains suggested in 2003 Resolution 2003/2032 (INI). This Resolution noted that, on account of the above agreements, the death of a Community citizen in a Member State other than his country of origin results in more complex procedures, a longer period of time before burial or cremation takes place and higher costs than if the death had occurred in the deceased person's country of origin,

Another compelling reason for this Resolution was the recognition that, in view of the growth in intra-Community tourism, the increasing numbers of retired people who choose to live in a country other than their own and, more generally, greater intra-Community mobility which is actually encouraged, the number of Community citizens who die in a country other than their country of origin was bound to increase. This was considered against the backdrop that Community citizens should, *mutatis mutandis*, be able to move between and reside in Member States in similar conditions to nationals of a Member State moving around or changing their place of residence in their own country, and that exercising the right to freedom of movement and freedom of residence should be facilitated to the utmost by reducing administrative formalities to an absolute minimum.

The European Community was of the view that, at the time the Resolution was proposed, it was still far from true that a Community citizen who dies in a Member State other than his own is treated in the same way as a national who dies in his home country. For, example, the fact that a zinc coffin is required for the

[107] Article 7 of the Strasbourg Agreement.

repatriation of a corpse from Salzburg to Freilassing (a distance of 10 km) but not for the transfer of a body from Ivalo to Helsinki (a distance of 1,120 km) (2).

Therefore it was pointed out that the repatriation of mortal remains without excessive cost or bureaucracy in the event of the death of a European Community citizen in a country other than the one in which either burial or cremation was to take place may be regarded as a corollary of the right of each EU citizen to move and reside freely within the territory of the Member States.

The Resolution called upon the Commission to see that the standards and the procedures applied in the cross-border transportation of corpses were harmonized throughout the Community and to endeavor to ensure that, as far as possible, Community citizens were treated in the same way as nationals in their home country.

A Regulation, covering intra-community transport of bodies according to the European Standard CEN/BT/TF 139 on Funeral Services and approved on 27 July 2005 goes on to say in Article 1 that the identification of the deceased must be performed before the body is placed in the coffin by the funeral enterprise or operator of the country of departure. The elements of identification relate to the civil status of the deceased and are indicated on the laissez-passer for the body. For identification, the body must be provided with: an identification bracelet attached to the body part (wrist, ankle. . .,); and a non-removable and tamper-proof identification tag attached to the coffin and its wrapping, if any. The information required on the bracelet were: surname and first name(s); sex; date and place of birth; date and place of death; and nationality. The information required on the identification tag were to be: surname and family name(s); date of birth; and date of death.

Article 2 of the Regulation required that the coffin or casket that carried the remains must be made of solid material—the main material used in Europe being wood (excluding the use of carton or chipboard). The material used for the coffin must be biodegradable. It also required that the coffin must be impervious; the products used to make it impervious must be biodegradable and in conformity with the standards applicable to crematorium emissions. In particular, the coffin must be impervious to decomposition liquids and fitted with absorbent material. The out cover of the coffin/casket was required to meet necessary sanitary requirements.

The Regulation had chemical requirements that were not contained in the 1937 Berlin Agreement and the 1973 Strasbourg Agreement. For instance, Articles 2.3 and 2.5, specified conditions for international carriage of corpses by providing that if the cause of death was a contagious disease (as per the WHO official list), the outer container (usually wooden) used for the transport of the body may be lined with a hermetically sealed container. The hermetically sealed container must be provided with a purifying filter. If the consecutive treatments (thanatopraxy) have been performed within 36 h after the death the body must be encoffined within 6 days. The transport must be done not more than 48 h after encoffining and sealing. The conditions required for long distance international transport outside Europe under the Agreement were: hermetically sealed container; and/or embalming/thanatopractical treatment; and/or refrigeration. In the case of refrigeration at no time shall the temperature inside the container exceed 80 °C during transport.

The Regulation requires two types of documents for carriage of corpses: medical certificate upon death; and a laissez passer. The medical certificate is required to be drawn up, on the one hand, in the language of the country of departure in which the death had occurred and, on the other hand, in one of the following languages: English, German or French. It must contain information relating to the deceased such as: surname and maiden name in the case of a married woman; first name(s); date and place of birth; date and place of death; sex; and cause of death.

6.3.3 ICAO Initiatives

The Council

The Council of ICAO, at its 32nd Session in 1957 addressed the carriage under the heading "Carriage of Sick Persons, Pregnant Women, Live Animals and Coffins—Sanitation on Board Aircraft" at which IATA recommended that in addition to the prevailing requirement—that human remains be placed in hermetically-sealed coffins which are enclosed in outside cases—human remains should be embalmed prior to being placed in the coffin. IATA further suggested that acceptance of such coffins is dependent upon the type of aircraft, requirements of entry and clearance and prior approval of the countries of origin, transit and destination.[108] The Council noted that comments on the carriage of coffins had been received from 27 States (from a total of 72 member States at that time) and two overseas territories. Three of these States reported that they were bound by the provisions of the 1937 Berlin Agreement and Eight States advised ICAO that the carriage of corpses existed in their national legislations. Thirteen States commented that they had not, in their experience encountered serious difficulties in this area. The United States made the comment:

> Because of known effects of rare atmosphere at high altitude on sealed caskets, such caskets should not be carried by aircraft.[109]

The ICAO Secretariat responded in assent:

> Differences in atmospheric pressure are known to have caused bursting of coffins, particularly when sealed hermetically (by welding) according to provisions of Articles 5 and 7 of the Berlin Arrangement, or similar provisions in national legislation. Prompted by rapid decomposition in flight, such transports occasionally arrive in appalling conditions; in some States (Australia, Philippines, Venezuela, Netherlands Antilles), therefore, it is required that corpses be embalmed prior to air transport, thus eliminating at least certain difficulties. If some pressure-relief system were applied to sealed caskets, the difficulties caused by pressure differences might disappear, but international transport would not permitted by existing laws.

[108] C-WP/2448, 5/6/57, Addendum and Corrigendum, 21/11/576 at 3.

[109] *Id.* Paragraph 20.1 at p. 10.

It is noteworthy that during these discussions, cremated human remains were not mentioned, except by Belgium which said that "incinerated corpses are accepted without any restrictions and are carried on all types of aircraft".[110] The ICAO Council concluded that the difficulties reported by States were caused by variations of atmospheric pressure; a characteristic of transport by air, while for international transport coffins must be hermetically sealed.

ICAO has approached this subject from another dimension *i.e*. the carriage of human remains of an aircraft accident victim. In 2001 the Council released its *Guidance on Assistance to Aircraft Accident Victims and their Families*[111] where ICAO recognizes that in an accident context the identification, custody and return of human remains are very important forms of family assistance but remains are often difficult to recover and identification can be an arduous and time consuming process. The ICAO guidance goes on to say that legislation often requires a post mortem examination of those killed in an accident and in some instances there may be remains that cannot be identified.[112] ICAO also calls for personal effects of the deceased to be correctly handled and returned to their lawful owners.[113] The Guidance also calls for the State of occurrence to provide for the return of human remains[114] while also devolving that burden—of the carriage of such remains—upon the aircraft operator involved in the accident.[115]

Annexes 9 and 18 to the Chicago Convention

There are two Annexes to the Chicago Convention which bear some relevance to the carriage of human remains by air—Annex 9 (Facilitation) and Annex 18 (The Safe Transport of Dangerous Goods by Air). The Annex 9 definition of cargo implies that human remains could be categorized as cargo by giving the definition of cargo as "*any property carried on an aircraft other than mail, stores and accompanied or mishandled baggage*". This definition is slightly different from the one contained in another ICAO document—*Technical Instructions for the Safe Transport of Dangerous Goods by Air*[116] which defines "cargo" as "*any property carried on an aircraft other than mail and accompanied or mishandled baggage*". Annex 18 does not define the word "cargo" but defines "dangerous goods" as articles or substances which are capable of posing a risk to health, safety, property or the environment and which are shown in the list of dangerous goods in the

[110] C-WP/2448, 5/6/57, Appendix "A" at 25.

[111] *Guidance on Assistance to Aircraft Accident Victims and their Families, ICAO Circular 285 – AN/166*.

[112] *Id*. Paragraph 3.10.

[113] *Id*. Paragraph 3.11.

[114] *Id*. Paragraph 5.1.

[115] *Id*. Paragraph 5.7.

[116] ICAO Doc 9284, AN/905 (2011–2012 Edition).

Technical Instructions or which are classified according to those instructions. The Technical Instructions do not list human remains as being dangerous cargo. However, it behooves the international aviation community to inquire, along the lines of ICAO discussions in the Council, whether human remains could be ruled out as not posing a risk to health or the environment under any circumstances of carriage by air or whether human remains, depending on the way it is packed for transport, could be considered as dangerous goods.[117]

Getting back to Annex 9, there is a whole chapter in the Annex—Chapter 4—dedicated to the entry and departure of cargo and other articles. Surprisingly, there is no provision in the Annex for priority of clearance or transport of human remains over other cargo, despite the prominence given to the subject in *ICAO Circular 285 – AN/166*.[118] Another surprise is that, although there is a *Recommended Practice* in the Annex which suggests that electronic information systems for the release and clearance of "goods" (my emphasis) should cover their transfer between air and other modes of transport,[119] there is no definition of "goods" in the Annex. Do corpses or cremated human remains come under the purview of "goods"? This question is valid in the context of Appendix 3 to the Annex which has a template for a cargo manifest where there exists a column for "Nature of Goods". There is no mention of the word "cargo" in this template.

In view of the above discussion it might be worthwhile for a detailed discussion on the status of human remains in the global aviation context and a re-visit of the 1957 discussions in the ICAO Council. The added dimension of related ICAO documentation such as Circular 285 – AN/166 makes it all the more compelling.

IATA, WHO and UNITED STATES Guidelines

The International Air Transport Association has clear, cogent guidance on the carriage by air of human remains. In its *Airport Handling Manual* (AHM) IATA prescribes that for special cargo, such as valuable cargo, perishables, vulnerable cargo, human remains and shipments of special importance or urgency, particular points to be considered are: that all personnel concerned are made fully aware of the nature and handling requirements of all such shipments; suitable arrangements are made for the security of valuable and vulnerable cargo; perishables are handled in accordance with the requirements of the particular commodity and in particular the most recent edition of the Perishable Cargo Regulations Manual; that a check is made to ensure that the final load assembled for dispatch to the aircraft *does* include shipments of special importance or urgency; and that shipments considered as

[117] American Airlines requires that human remains packed in dry ice are subject to dangerous goods regulations. https://www.aacargo.com/shipping/humanremains.jhtml.

[118] *Supra* note 111.

[119] Annex 9 to the Convention on International Civil Aviation, 13th Edition: July 2011, *Recommended Practice* 4.18.

special cargo have "special consignment" labels visibly attached to each package.[120]

The *IATA Ground Operations Manual* (IGOM) provides that human remains should be carried in an aircraft only if accepted by the operating airline for transport. The IGOM requires the carrier to make sure that a Human Remains Acceptance Checklist has been used (if required by the operating airline). Carriers are required, according to the IGOM, not to accept any human remains that are consolidated with any cargo other than other human remains. With regard to cremated human remains the Manual requires that only urns or other suitable containers as cargo with no special restrictions are accepted for carriage and that the carrier should make sure that the urn or other container is packed in a neutral outer pack that will protect the urn from breakage and/spillage.[121] It also prescribes that human remains in coffins should not be stored next to food or live animals, adding that there appears to be no scientific or technical reason why live animals and human remains should be segregated in aircraft cargo compartments, except that it may be ethical for cultural reasons to segregate them.

IATA in AHM 333 states that, should a body fluid leakage occur while transporting dead bodies, the usual accepted guidelines endorsed by WHO for dealing with spilled body fluids should be followed and the handler is advised to: wear disposable gloves and, if available, a plastic apron. If the spillage has occurred on an aircraft, the AHM provision advises the handler to only use cleaning materials suitable for aircraft use. He should not try to clean the body fluids by hosing with water or air and should use material that will adsorb the body fluids and scrape the material into a biohazard bag. Afterwards, he should wash the area with water/disinfectant after removal of the adsorbent material, dispose of gloves and apron in a biohazard bag and wash hands thoroughly with soap and water afterwards.

WHO has also some guidance pertaining to the handling of human remains, and recommends as a fundamental measure that the handling of human remains should be kept to a minimum. Additionally, WHO recommends, particularly in the case of deaths caused by infectious diseases that remains should not be sprayed, washed or embalmed and that only trained personnel should handle remains during the outbreak. Personnel handling remains should wear personal protective equipment (gloves, gowns, apron, surgical masks and eye protection) and closed shoes.[122]

In the United States, there are no requirements for importation into the country if human remains consist entirely of: clean, dry bones or bone fragments or human hair; teeth; fingernails or toenails; and human remains that are cremated before entry into the United States. Human remains intended for interment or subsequent cremation after entry into the United States must be accompanied by a death

[120] IATA Airport Handling Manual, AHM 310 at 149.

[121] IATA IGOM, Chapter 3.

[122] Interim Infection Control Recommendations for Care of Patients with Suspected or Confirmed Filovirus (Ebola, Marburg) Haemorrhagic Fever, BDP/EPR/WHO, Geneva, March 2008.

certificate stating the cause of death. If the death certificate is in a language other than English, then it should be accompanied by an English language translation.

If the cause of death was a quarantinable communicable disease (i.e., cholera, diphtheria, infectious tuberculosis, plague, smallpox, yellow fever, viral hemorrhagic fevers, SARS, or pandemic influenza), the remains must meet the applicable standards and may be cleared, released, and authorized for entry into the United States only if: the remains are cremated; or the remains are properly embalmed and placed in a hermetically sealed casket; or the remains are accompanied by a permit issued by the Director of the Centre for Disease Control and Prevention (CDC). The CDC permit (if applicable) must accompany the human remains at all times during shipment. If the cause of death was anything other than a quarantinable communicable disease, then the remains may be cleared, released, and authorized for entry into the United States if: the remains meet the standards for applicable or properly embalmed and placed in a hermetically sealed casket, or are accompanied by a permit issued by the CDC Director; or the remains are shipped in a leak-proof container.

Federal quarantine regulations (42 CFR Part 71) state that the remains of a person who is known or suspected to have died from a quarantinable communicable disease may not be brought into the United States unless the remains are; properly embalmed and placed in a hermetically sealed casket, cremated, or accompanied by a permit issued by the CDC Director. Quarantinable communicable diseases include cholera; diphtheria, infectious tuberculosis; plague; smallpox, yellow fever; viral hemorrhagic fevers (Lassa, Marburg, Ebola, Congo-Crimean, or others not yet isolated or named); severe acute respiratory syndrome (SARS); and influenza caused by novel or re-emergent influenza viruses that are causing or have the potential to cause a pandemic. A CDC permit may be required when the remains are not embalmed or cremated, especially if the person is suspected or known to have died from a communicable disease.

Persons wishing to import human remains, including cremated remains, into the United States must obtain clearance from CDC's Division of Global Migration and Quarantine (DGMQ). Clearance can be obtained by presenting copies of the foreign death certificate and if needed, a CDC/DGMQ permit to the CDC Quarantine Station with jurisdiction for the U.S. port of entry. A CDC/DGMQ permit may be needed to import human remains if the deceased is known or suspected to have died from a quarantinable communicable disease. A copy of the foreign death certificate and the CDC/DGMQ permit must accompany the human remains at all times during shipment. The foreign death certificate should state the cause of death and must be translated into English.

The basic principle that should apply to the handling of human remains must be consistent with the policy which currently applies in case of aircraft accident investigations, in that the country in which the death occurred must act contemporaneously and in close consultation with the country of nationality. This would obviate the case of the British tourist who died in Greece. The second principle should be that the principles of *ICAO Circular 285 – AN/166* should be incorporated into Annex 9 along with a Standard in Chapter 4 that human remains should

be accorded priority and dignity and that specially reduced rates should be promulgated by States on their airlines for this purpose. This Standard should be adopted in accordance with the basic philosophy of Article 44 d) of the Chicago Convention which states that ICAO should strive to meet the needs of the people of the world for safe, regular, efficient and economical air transport.

Annex 9 should contain a separate Appendix for the carriage of human remains by air, which would lay down global principles for the handling, care and commitment that States could ensure. This Appendix should have a cross reference to Annex 18 and the *Technical Instructions* contained in Doc 9284[123] with appropriate linkages that ensure the harmonious application of both Annexes to this sensitive subject.

As for Annex 18, a study should be undertaken to determine as to when a cadaver or cremated remains would, if at all, become a dangerous good. The focus area would be both on the condition the human remains are at the point of acceptance for carriage, and the manner in which they are packaged. In the ultimate analysis, there has to be core global rules in place for this important area of air transportation. It cannot be left for individual States or airlines to decide.

Enhancing global civil aviation security and facilitation is one of ICAO's Strategic Objectives as adopted by the Council in May 2012. This is the first time facilitation has been mentioned in ICAO's strategic language and it should be a harbinger of new studies and new cooperation with the international community between ICAO and its member States o the carriage by air of human remains.

References

Abeyratne RIR (1992) The development of the machine readable passport and visa and the legal rights of the data subject (Part II). Ann Air Space Law (Annales de Droit Arien et Spatial) XVII:1–31

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 (2002b) Attacks on America – privacy implications of heightened security measures in the United States, Europe, and Canada. J Air Law Commerce 67(1):83–115

Abeyratne RIR (2003) Profiling of passengers at airports – imperatives and discretions. Eur Transport Law XXXVIII(3):297–311

Abeyratne RIR (2010) The NW 253 flight and the global framework of aviation security. Air Space Law 35(2):167–181

Becker T (2006a) Terrorism and the state, Hart monographs in transnational and international law. Hart, Portland, p 155

Becker T (2006b) Terrorism and the state; rethinking the rules of state responsibility. Hart, Portland

Bennet CJ (1992) Regulating privacy. Cornell University Press, Ithaca, p 13

[123] *Supra* note 116.

Blackstone W, Morrison W (eds) (2001) Commentaries on the laws of England (1765–1769), 4th edn. Cavendish, London, p 68
Brownlie I (1983) System of the law of nations: state responsibility, Part 1. Clarendon, Oxford, p 39
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. Transnational Publishers, Irvington-on-Hudson, p 109
Cate FH (1997) Privacy in the information age. Brookings Institution Press, Washington, p 49
Cooley TM (1888) A treatise on the law of torts, 2nd edn. Callaghan, Chicago
de Arechaga EJ (1968) International responsibility. In: Sorenson M (ed) Manual of public international law. St. Martin's Press, New York, p 531
De Vattel E, Fenwick CG (tr) (1916) The law of nations or, the principles of natural law: applied to the conduct and to the affairs of nations and sovereigns, 2nd edn. Legal Classics Library, New York, p 72
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, 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. Georgia Law Rev 12:423
Gavison R (1980) Privacy and the limits of the law. Yale Law J 89:421
Goff S (2013) The insider threat to airport security, 14 March 2013. http://strategicstudyindia.blogspot.ca/2013/03/the-insider-threat-to-airport-security.html
Grotius H, Scott JB (tr) (1646) De Jure Belli Ac Pacis 2: 523–526
Halpin A (1997) Rights & law analysis & theory. Hart, Oxford, p 111
Hoffer S (2000) World cyberspace law. Juris Publishing, Huntington
Hoffman LJ (ed) (1980) Computers and privacy in the next decade. Academic, New York, 142
Honig JP (1956) The legal status of aircraft. Martinus Nijhoff, The Hague, p 29
Hyde C (1928) Concerning damages arising from neglect to prosecute. Am J Int Law 22:140
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, Brussels, 30 September–3 October 1970, Manchester University Press, Manchester
McMunn MK (1996) Aviation security and facilitation programmes are distinct but closely intertwined. ICAO J 51:9
Miller AR (1971) The assault on privacy. The University of Michigan Press, Ann Arbor, p 42
Montgomery Curtis J (1992) Memorial seminar. The public, privacy and the press: have the media *gone too far?* American Press Institute, p. 2
Morganthau H, Thompson KW (1950) Principles and problems of international politics. Knopf, New York, p 24
Nock SL (1993) The costs of privacy. Aldine De Gruyter, New York, p 43
Orwell G (1978) 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. Georgia 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, p 33
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
Rucker P (2010) TSA tries to assuage concerns about full body scans. Washington Post, Monday, 4 January 2010

Scott GG (1995) Mind your own business – the battle for personal privacy. Insight Books, New York, p 307
Shaw MN (2003) International law, 5th edn. Cambridge University Press, London, pp 611–612
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, p 71
Sweet K (2008) Aviation security and passenger rights. In: Thomas AR (ed) Aviation security management, vol 2. Praeger Security International, Westport, p 45
Turack DC (1972) The passport in international law. D.C. Heath & Co., Lexington, pp 20–21
Warren SD, Brandeis LD (1980) The right of privacy. Harv Law Rev 4(5):193
Warren SD, Brandies LD (1980–1981) 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, London, p 124
Young JB (1978) A look at privacy. In: Young JB (ed) Privacy. Willey, New York, p 1
Zelermyer W (1959) Invasion of privacy. Syracuse University Press, Syracuse, p 16