PRIO

Data Protection and Security in Civil Aviation

Despite the massive attention generated by the events of 11 September 2001, terrorist threats are not the sole issues of concern to the aviation industry, which must also address challenges presented by a range of other issues, including serious crime; attacks on the data integrity of communications networks; attacks on information and personnel management systems; chemical, biological, radiological and explosive threats, etc. However, implementation of most of the security measures that have already been put into practice or are currently being planned has generally taken place under the rubric of combating terrorism.

Olga Mironenko *Faculty of Law, University of Oslo)*

Aviation security: background and legal framework overview

Initially, international surveillance mechanisms in the civil aviation sector were quite general and rather limited. The Chicago Convention (1944) established the International Civil Aviation Organization (ICAO), a specialized agency of the United Nations charged with coordinating and regulating international air travel. After the world was first confronted with the problem of politically motivated aircraft terrorists in the late 1960s, the ICAO adopted Chicago Convention Annex 17 – Security (1974), which established the foundations of an international aviation security programme and sought to safeguard civil aviation against acts of unlawful interference.

At the same time, many countries, including the USA, introduced measures such as pre-flight and luggage controls on a national basis. The level of security demands grew constantly, however, which resulted in security measures becoming increasingly sophisticated. For example, in the late 1990s, the Computer Assisted Passenger Prescreening System (CAPPS) was created in the USA, which made it possible to automatically single out particular passengers and put them through stricter security controls.

The US Aviation and Transportation Security Act (2001) was enacted immediately after the attacks of 9/11. Numerous countries, including Canada, China, the United Kingdom, France, Russia, Germany, India and Pakistan, also introduced new anti-terrorism legislation in the wake of the attacks. In addition, the European Union (EU) adopted its first set of common rules in the field of civil aviation security, which EU/European Economic Area (EEA) member-states are obliged to follow (Regulation EC No 2320/2002). Amendment 10 to Annex 17 was adopted by the ICAO on 7 December 2001 in order to address challenges posed by the events of 9/11.

Since 1974, the provisions of Annex 17 – Security have been revised and updated eleven times. The ICAO has also adopted legal and technical regulations and procedures designed to prevent and suppress acts of unlawful interference; has produced guidance material to assist with the implementation of security measures (the Security Manual for Safeguard-ing Civil Aviation Against Acts of Unlawful Interference, Doc 8973 – Restricted); and has issued Standards and Recommended Practices (SARPs). The ICAO's work in the field of security is carried out in three areas: policy initiatives, audits of the organization's 190 contracting states, and assistance to states that are unable to address serious security deficiencies highlighted by audits.

However, the ICAO's regulations, guidelines and SARPs are recommendations only: contracting states are not obliged to comply with them (although they are obliged to report deviations), and there are no enforcement mechanisms. Thus, efforts to develop global standard approaches in this area are facing major challenges. Airlines and other participants have to deal with a range of different systems, each with different requirements and procedures. This creates technical and operational chaos, with substantial financial consequences.

Security measures to prevent terrorist acts in Norway have almost exclusively been implemented as a consequence of international regulations. As a member of the EEA, Norway is bound by the EU legislation incorporated in the 1992 Agreement on the European Economic Area. It is therefore bound by the EU common rules in the field of civil aviation security, which have been incorporated into the Norwegian legal system (Lov om luftfart, 1993, Forskrift om sikkerheten i Luftfarten, 2004). In addition, much Norwegian security legislation is connected to the country's participation in the Schengen Area cooperation. There have been few independent Norwegian initiatives on anti-terrorist security measures.

Security measures

New technologies, systems and security devices aimed at enhancing security standards, preventing attacks and ensuring surveillance are now appearing every day. These include: intensified security checks of passengers and luggage; camera surveillance and use of closed-circuit television (CCTV); security measures based on biometrics (photographs, DNA and fingerprints); scanners, including whole-body scanners; transfer of air passenger data from airlines to state authorities, etc.

Most of the new measures are being implemented and enhanced in response to situations that have already occurred. Following the first cases in which terrorists attempted to carry weapons made of metal, such as knives and guns, states installed metal detectors. After 9/11, among other things, the USA demanded that all international airlines have to provide the US government with Passenger Name Records (PNR). This meant complete electronic access to detailed airline passenger data on all travellers registered in the airlines' computer systems. Since the so-called shoe bomber attempted to hide explosives in his shoes in December 2001, states have made travellers remove their shoes during security checks. The transfer of Advanced Passenger Information (API) by the airlines to the states was implemented in the EU after the terrorist attacks in Madrid in 2004. In 2006, an alleged attempt to use liquid explosives on board aircraft led to measures prohibiting passengers from carrying liquids onto aircraft. Just a few days after car-bomb attacks in Glasgow and London in June 2007, the EU announced a project containing anti-terrorism measures, including the creation of a European PNR system. On 25 December 2009, the so-called underwear bomber attempted to detonate plastic explosives hidden in his underwear, and many states have since sought to install whole-body scanners (although it should be noted that the 'underwear bomber' boarded his US-bound flight at Amsterdam's Schiphol Airport, which already has 15 body scanners. Scanner manufacturers have also admitted that their equipment would not have detected the underwear bomb because the explosives were in a light powdered form and the detonator was hidden in a body cavity).

It is commonly accepted that effective security must be ensured in the aviation sector, but it remains questionable whether the new measures and technologies actually promote security. According to a number of surveys, there are doubts as to whether the measures add value to the fight against terrorism and crime, while it is quite obvious that the current regime is exposing air passengers to increasing restrictions and humiliations.

In any event, air-travel security measures cannot simply be considered mere technical measures related to aviation security, as some of them have a serious impact on issues of

human fundamental rights, which are protected by law nationally and internationally.

Impact on human rights

Measures – such as checking bags for bombs, strengthening cockpit doors and placing air marshals on flights – that do not infringe upon individual privacy may be considered sound security measures. Other measures, however, may present risks to the privacy and security of individuals because they may infringe passengers' right to privacy and dignity, create data files directly linked to the identity of air travellers, violate freedoms of thought, conscience and religion, as well as the principle of non-discrimination, the rights of children, etc. For example, the collection of passengers' personal data by airlines and subsequent transfer of such data to state authorities in many cases conflicts with data-protection requirements, while implementation of CCTV, use of biometrics and 'pat-down' searches also raise privacy and civil liberties concerns. Currently deployed whole-body scanning devices produce black and white images of the human body with blurred faces. But they still reveal a person's gender, the precise construction of the body and very sensitive areas of a person's private life, medical aids and conditions . The use of scanners may be thus equivalent to a virtual strip search (backscatter x-ray or millimeter-wave scanning machines are currently in operation in the USA, the UK, the Netherlands and many other countries). Moreover, it is uncertain whether the machines may have a possible adverse impact on passengers' health, owing to potential radiation hazards. State authorities and manufacturers claim that the scanners deliver a 'safe' dose and are not harmful for the frequent traveller, but it is probably too early to predict the long-term effects.

With the exception of human rights that cannot be derogated for reasons of national security under any circumstances (peremptory norms or *jus cogens*), the United Nations recognizes that human rights can be limited or even pushed aside during times of national emergency. But, what about the rights of everyday travellers? Regulate checks in airports or routine transfer of passengers' personal data by airlines to government agencies can hardly be seen as national emergency situation undertakings.

Is it possible to find an appropriate balance between the need for surveillance and privacy-related interests?

The solution and problems

The point is that breaching people's rights and freedoms can be justified under human rights legislation, if it is done in accordance with the law and is proportionate and necessary for national security, public safety and for the protection of the rights and freedoms of others. But every security measure has to be clarified, justified and accompanied by strong and adequate safeguards, procedures and rules that satisfy and ensure human rights standards and requirements. In addition to legal norms establishing such safeguards, the means for ensuring their effective application should also be determined. It is important to ensure that all actors implement the regulations, practices and measures in reality. But, how can this be done in practice?

As already noted, the ICAO has limited possibilities for establishing and enforcing common rules at the global level, owing to the organization's advisory nature. As for the EU, the USA and the national level in general, there appear to be numerous political issues and policies that have considerable impact upon security and privacy regimes. Many of the decisions and rules related to security, including legal frameworks and international agreements, are based on political approaches and are often therefore more political solutions than legal instruments. Even when steps are taken to protect human rights, these are not necessarily effective, and they may be characterized by weaknesses, shortcomings and contradictions.

For example, when a conflict arose between the USA's request for PNR transfer and EU

data-protection requirements, the parties attempted to reach an agreement on data transfer in a series of bilateral agreements (in 2004, 2006 and 2007). The deal gave rise to widespread privacy and security concerns. Although the two sides tried to provide 'safeguards', the agreement in fact failed to offer an adequate level of data protection and left many problems outstanding. Nevertheless, since then, the EU has been establishing its own PNR system using the controversial EU–US PNR agreement of 2007 as a model.

How a particular security measure is described, which of its aspects are seen as central and which viewed as marginal, is a crucial concern . For example, should the transfer of personal data be primary understood as a security measure, or as a human rights question? What will be considered more important: the need for surveillance, or privacy-related interests? No doubt, the core values will be security for security organs, and human rights for human rights organs.

For those who question the legality of particular security measures, the most central issue is often the violation of human rights. It is claimed that we are undermining our privacy, dignity and individualism on the stage of security theatre, in the name of a goal of total safety through technology. For governmental institutions, however, the most central issue would seem to be public and state security and defence. The USA, for instance, regularly insists that existing measures are insufficient to fight terrorism. One of the US bill proposals regarding whole-body scanning states: 'It is the policy of the US to aggressively seek, develop, and deploy, in a timely fashion and sufficient numbers, primary screening technologies capable of detecting and protecting against threats to domestic and international aviation travel that cannot be effectively and efficiently detected by other technologies currently more commonly utilized in airports.' Recent developments have shown that other countries' security policies are greatly influenced by developments in the USA.

Although different governmental agencies seem intent on trying to convince the public that air-travel security measures are 'non-invasive' and 'protect your privacy', closer examination usually reveals the opposite. Both the measures and the 'safeguards' proposed by security agencies have come under constant fire from a range of institutions and advocacy groups concerned about human rights, and there seems to be no sign of either side giving up its position in the immediate future. However, the fact that states possess political and economic power and flights apparently must go on renders issues of privacy dependent on economic and political needs.

It may therefore be extremely difficult to find a solution through the introduction of adequate safeguards, especially internationally. The control and surveillance regime that is designed to uphold security and prevent terrorism and crime will most likely prevail over human rights issues. As a result, there continues to be a major risk of significant losses of liberty, privacy, individualism and dignity on the part of citizens.

There has been some public discussion of possible alternative solutions, such as focusing on proactive intelligence instead of reacting to past situations; a shift to less invasive technologies and/or effective 'lo-tech' solutions; handing control of security back to the airlines; training ordinary citizens to stop terrorists on airplanes; forget about privacy at all; or, finally, simply refusing to fly whenever possible.

Achieving the right balance between the need for security measures and issues related to human rights is a matter of public concern, interest and dispute, both internationally and at the national level. The issue is relevant to state and public institutions, private companies and, finally, every individual who can see themselves travelling by means of air transportation. In a global sense, security/privacy issues that might first appear in the context of civil aviation often go further and spread into many other spheres. Thus, issues currently being raised in relation to air travel can become even more important and challenging over time.

The ICAO's role should be revised, so that it might be enabled to establish and enforce global common rules and standard approaches in civil aviation, particularly in relation to ensuring passengers' rights.

States should suspend implementation of new security measures until a comprehensive evaluation of their effectiveness, health impacts and privacy safeguards has been completed by an independent board of review. Thorough justification should be given before the introduction of any new security measure, and substantial evidence should be presented to show that the measure is proportionate, necessary and adds value to already existing security measures.

Increased usage of information, telecommunication and other technologies requires further development of legislation to specify necessary terms and rules.

Mechanisms should be established to enable individuals to enforce their rights, such as the right to view and correct data kept about them by state authorities. An option of alternative security methods should be developed and made available to passengers with 'privacy concerns'. States should concentrate on developing alternative solutions that are non-invasive or less invasive for passengers.

Passengers should be provided with appropriate, comprehensive and clear information about all applicable security measures – along with information regarding the protection of their rights – before travelling and before purchasing the tickets, at airports, and while they are on board an aircraft. This would at least enable them to make a informed decision on whether they wish to waive their rights.

THE AUTHOR

Olga Mironenko is a PhD Candidate at the Norwegian Research Center for Computers and Law, University of Oslo. She holds a diploma in law from the State University – Higher School of Economics in Moscow and an LLM from the University of Oslo in Information and Communication Technology Law. She formerly worked as a lawyer in the civil aviation industry in Russia.