DATA PROTECTION AND SECURITY IN CIVIL AVIATION

Olga Mironenko
21 March 2010
University of Oslo
Introduction

• The right to privacy and data protection are fundamental human rights.
• Effective security must be ensured in the civil aviation sector. Such security measures as body scanners installed at airports and collection and transfer of air passenger data from airlines to the state authorities are intended to keep a high level of security and protect our lives.
• These measures have a serious impact on privacy and data protection.

↓

A conflict arises between the use of these security measures and the protection of these rights.
Dilemma

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

• Is it possible to reach a situation when the persons’ rights to life and safe travelling would not be in conflict with their rights to privacy and data protection?
Background

- 1900s – first aircrafts
- Chicago Convention (1944) - the International Civil Aviation Organization (ICAO)
- Hijacking as a threat for civil aviation (1968)
- National measures - pre-flight and luggage controls
- 11 September 2001 in the US
- The US Aviation and Transportation Security Act (2001)
- Anti-terrorism legislation in Canada, China, the UK, France, Russia, Germany, India, Pakistan, etc.
- EU - first common rules in the field of civil aviation security (Regulation EC No 2320/2002), Amend.10 to Annex 17 by ICAO
Apart from terrorist threat:

• serious crime
• attacks on the data integrity of communications networks
• attacks on the information and personnel management systems
• chemical, biological, radiological, and explosive threats, etc.
Security measures

• lots of new technologies, systems and security devices aimed at enhancing security standards
• intensified security checks of passengers and luggage
• camera surveillance and Closed-Circuit Television (CCTV)
• biometrics (photographs, DNA and fingerprints)
• scanners, including whole-body scanners
• transfer of air passenger data from airlines to the state authorities, etc.
Security measures as a reaction to past situations

- Weapons made of metal → metal detectors
- 9/11 → Passenger Name Records (PNR) system in US
- December 2001 shoe bomber → take off shoes
- 2004 attacks in Madrid → transfer of Advanced Passenger Information (API) in the EU
- 2006 liquid explosives → prohibition of liquids
- 2007 car bomb attack → EU PNR system project
- 25.12.2009 underwear bomber → whole-body scanners
Impact on human rights

- Right to privacy
- Right to personal dignity
- Data protection
- Freedoms of thought, conscience and religion
- Non-discrimination
- The rights of child
- Impact on health
- etc.
The solution

• Security measures must be accompanied by strong and adequate safeguards which satisfy and ensure the human rights requirements.

• All aviation security measures should respect the principle of proportionality as justified and necessary in a democratic society.

• In addition to legal norms, the means for ensuring their effective application should be established as well. It is important that all actors implement the regulations, practices and measures.
ICAO

• Annex 17 – has been updated 11 times since 1974
• Legal and technical regulations and procedures to prevent and suppress acts of unlawful interference
• The Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (guidance material to assist with the implementation of the security measures)
• Standards and Recommended Practices (SARPs)
ICAO’s work in the field of security

*Three areas:*

- policy initiatives
- audits of its 190 contracting states
- assistance to states that are unable to address serious security deficiencies highlighted by audits
ICAO’s regulations, guidelines and Standards and Recommended Practices (SARPs)

• According to the text they are mandatory for contracting states
• the states are obliged to report about deviations
• **BUT** there are no enforcement mechanisms

↓

Endeavors to make global standard approaches are facing major challenges
Air passenger lists

• The initial purpose of collecting passenger data by the airlines is to document commercial air transportation.

• 1944 - Chicago Convention. Art.29 requires every aircraft to carry certain documents, including, for passengers, “a list of their names and places of embarkation and destination”.

• 1990s - Computer Assisted Passenger Prescreening System (CAPPS) in the USA


• 2001- The US Aviation and Transportation Security Act - the Passenger Name Records (PNR) system. All international airlines had to provide the USA with electronic access to data on all travelers registered in the airline's computer system.
• 2003 - CAPPS II
• 2004 - Secure Flight
• 2004, 2006, 2007 - agreements on PNR transfer between the European Union (EU) and the USA
• 2006 - PNR agreement between the EU and Canada, 2008 - between the EU and Australia
• Some countries are also using PNR data (New Zealand, South Korea, Japan), within the EU – the UK has a PNR system.
• Many European states have enacted primary legislation on PNR or are testing using PNR data, and other countries are considering the use of PNR
• 2007 - Proposal of the European PNR system
<table>
<thead>
<tr>
<th><strong>Advanced Passenger Information (API)</strong></th>
<th><strong>Passenger Name Record (PNR)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collected on behalf of governments</td>
<td>Airlines collect PNR for their own needs</td>
</tr>
<tr>
<td>Serve border control and immigration purposes</td>
<td>Initially served commercial purposes</td>
</tr>
<tr>
<td>Derive from travel documents information (machine readable zone of a passport)</td>
<td>All the data that the passenger submits to the reservation system (up to 60 fields). May include sensitive data. Data cannot be deleted, even if cancelled. The system is not restricted to a specific flight. Include data on other customers.</td>
</tr>
<tr>
<td>Contain only validated biographical data</td>
<td>Completeness or accuracy not guaranteed. May not be fully updated on the date of departure.</td>
</tr>
<tr>
<td>The data is captured by the carrier prior to the departure</td>
<td>PNR may be created in a reservation system up to 360 days in advance</td>
</tr>
<tr>
<td>API records are created for each passenger</td>
<td>May include multiple passengers within the same record; data on several people: traveler, agent, staff, person paying for the ticket...</td>
</tr>
</tbody>
</table>
Global Distribution Systems (GDS)

- GDS book and sell tickets for multiple airlines.
- There are four major GDS platforms in the world: Amadeus, Sabre, Galileo and Worldspan.
- Amadeus is the only one of these that is based in the EU rather than the US.
- Each of them has a web site that gives anyone access to PNR data, very often with no password at all, but merely by reference to the reservation number printed on every ticket.
API

**International regulation:** API Guidelines by WCO, IATA and ICAO (2003)

The API should be limited to the data contained in the machine readable zone of travel documents or obtainable from existing government databases, such as databases containing visa issuance information.

**Problems:** There are no enforcement mechanisms.

- Many of API systems have been established hastily and impose data transmission requirements with minimal notice, without consideration of the technical, financial and operational aspects.
- Air carriers are required to comply with diverse requirements.
- Not all countries have passports that are machine readable.

API - USA

- name, date of birth, gender,
- citizenship,
- country of residence,
- travel document type, its number, expiration date, country of issuance,
- foreign registration number (if applicable),
- address while in the US,
- passenger contact information (phone),
- any other data deemed necessary to identify the persons traveling.

Some items are not in the machine readable zone of a passport
Main legal privacy framework

- Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (applicable in the EU);
- Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (not self-executing: it obliges members of CoE to incorporate its principles into their national legislation. It is open for ratification by states other than members of CoE);
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data (it is binding for EU/EEA member states);
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23.09.1980 (not legally binding on OECD members);
Data protection principles

• *Collection limitation principle:* Personal data must be collected and processed fairly and lawfully and kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

• *Data quality:* must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, be accurate, kept up to date.

• *Purpose specification:* must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

• *Use limitation:* should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with purpose specification principle except with the consent of the data subject or by the authority of law.
• **Security and confidentiality:** Collected data should be kept secure from any potential abuses.

• **Transparency and data subject participation:** Data subjects should be informed of the data processed, purposes of such processing and the identity of who is collecting their data. They should be allowed to access their data and make corrections to any inaccurate data.

• **Accountability:** Data subjects should have a method available to them to hold data collectors accountable for following the above principles.

• **The transfer of personal data from the EU/EEA to the countries lacking adequate level of protection is prohibited.**
Protection afforded by the USA

- The USA is not legally bound by any of the international data protection instruments.
- In the USA the right to privacy is protected by common law mechanisms.
- Privacy Act of 1974 protects personal information only when it is processed by the federal government.
- The USA has no general law protecting the privacy of “commercial” data.
- The airlines could allow the US government agencies to look at the data without the knowledge or consent of the data subjects.
- The USA cannot be considered as a country with adequate level of data protection.
PNR transfer between the EU and the USA

• The US’ request for PNR transfer after 9/11 became in conflict with the EU data protection requirements.
• Differences between the US and the EU legal systems and traditions.
• The airlines could allow the US government agencies to look at the data without the knowledge or consent of the data subjects.
As the result:

After the introduction of the new security measures in the USA, the European airlines found themselves in a difficult situation:

- refuse to transmit the data, thereby becoming subject to US authorities’ sanctions
- deliver the data in violation of the EU law

?

• The negotiations were pushy on the US side of the table.
• Despite the parties tried to provide “safeguards”, the agreement failed to offer an adequate level of data protection and left many problems open.
• The agreement was needed ASAP to avoid legal uncertainties for the EU member states, passengers and carriers, thus it was preferable to have an agreement with weaknesses and shortcomings, rather than not to have one at all.
• The agreement was more a political solution than a legal instrument.
• The deal provoked widespread privacy and security concerns.
• US is still trying to dictate tougher restrictions and get additional data from EU member states individually.
The weakest points of the Agreement:

- legal force and effect
- inadequate data protection standards
- scope of the agreement uncertainty
- lack of purpose limitation
- “pull”/”push” system issues
- unclear joint review procedure
- extended retention period
- enlarged list of data fields
- sensitive data issues
- no clear list of US authorities entitled to access PNR
- problem of enforcement of rights by the EU citizens
- dependence on change in the US legislation, *etc.*
Proposed European PNR System

• Decentralized system of data collection
• Passenger Information Unit (PIU) as recipient of the data in each member state, with “push” method used
• 19 PNR data elements
• Flights to/from the EU, excluding intra-EU and domestic flights
• Two data transmissions: one 48 hours before the flight takeoff and one when the flight has completed boarding
• 3 years in an active database and for a “further period of [not more than seven] years” in a dormant database
• Airlines refusing to provide the requested data before take-off will face withdrawal of their landing authorization
• It is not mentioned but EU-USA PNR scheme is used as a model
Criticism

• No substantial evidence is actually given that the collection of passenger data is necessary and adds value to the fight against terrorist offences and serious crime.

• Unclear relationship with other measures, such as Electronic System for Travel Authorization (ESTA), biometrics in passports, Schengen Information System (SIS), Visa Information System (VIS), national border protection schemes.

• Reports published by other agencies which had previous experience with PNR, such as the Government Accountability Office in the US, Germany and the UK did not confirm the efficiency of the measures.

• The text extends the aims of PNR processing.

• Same weaknesses as in the EU–USA agreement.
Real-world experiences

• Real-world experiences undertaken to see if a person can really be informed of his or her records that are being kept and processed proved that no one can rely on existing compliance, enforcement, or oversight mechanisms:
  • The request to the US Department for Homeland Security from a member of European Parliament Sophia In 't Veld to receive PNR information pertaining to her (2007).
  • The request to KLM Airlines from an American privacy advocate Edward Hasbrouck to see the records of his trip from the US to the EU and back (2007).
Conclusion

• Air passenger data have already become one of the most important sources for surveillance in the air traffic.
• There are doubts about whether the collection of data is necessary and adds value to the fight against terrorism/serious crime.
• ICAO’s Guidelines are not binding and they deal insufficiently with data protection issues.
• Even if some protection to human rights is given, it is not necessary effective; there may appear weaknesses, shortcomings and contradictions.
• Political issues and policies which effect the security and privacy regimes greatly. A lot of the decisions and rules are based on political approaches and are therefore more political solutions rather than legal instruments.
BODY SCANNERS

• 1992 - The first body scanner was created by Dr. Steven Smith in the USA - a technology that is capable of detecting objects carried under clothes.

• 2007 - The first airport with body scanners – Schiphol in the Netherlands.

• 25 December 2009 - “underwear bomber”.

• The list of airports currently deploying scanners is constantly growing and includes airports in the USA, the UK, Russia, etc.

• They are deemed to be one of the technical solutions required to keep a high level of security and intended to protect our lives.

• They have a serious impact on privacy and data protection as well as other fundamental rights and health.
Several technologies have been developed:

- X-ray backscatter
- Active millimeter wave
- Terahertz waves
- X-ray transmission imaging technology
Regulation

• The ICAO does not give any guidance on scanners.
• The usage or non-usage of the devices is based on the decision of a particular state.
• No common definition of a “body scanner”. Various terms are in use, such as “security scanner”, “whole-body scanning”, “advanced imaging technology”, “naked scanners”, “digital strip searchers”, etc.
The USA

- The Transportation Security Administration (TSA) began deploying advanced imaging technology in 2007.
- There are currently 486 imaging technology units at 78 airports.
- By 2014 the USA plans to deploy 1800 scanners in order to gradually introduce them as a primary screening method.
- There are several locations already where the scanners are used for primary screening, for example, Miami International Airport.
• 22 April 2009 - the US House of Reps passed “Aircraft Passenger Whole-Body Limitations Act of 2009”.


• Opinions of opponents receive wide coverage in the press and Internet (for ex., the incident in San Diego on 13.11.2010).

• On 2 July 2010, EPIC filed a lawsuit to suspend the deployment of body scanners at US airports.
The European Union (EU)

- The use of scanners is not currently regulated at the EU level.
- Member states may introduce the use of the scanners at their airports either by exercising their right to apply security measures that are more stringent than existing EU requirements or by exercising their right to conduct trials of new technical processes or methods for a maximum period of 30 months.
- 5 September 2008 the European Commission proposed a draft regulation including basic screening requirements to be further developed in legislation.
• 23 October 2008 – Resolution of the EP requesting the Commission to carry out an impact assessment
• 15 June 2010 - the Commission’s Report which assesses the current situation with regard to the use of security scanning technology in terms of detection capacity, and compliance with fundamental rights and health protection regulations
• Formal trials of scanners were undertaken in Finland, the UK, the Netherlands, France, Italy and Germany
• The UK intends to deploy scanners at all UK airports
• Finland and Italy – decided to discontinue the use of scanners
Human rights concerns

The use of body scanners has an impact on fundamental human rights enshrined in different human rights conventions, such as the Universal Declaration of Human Rights of 1948:

• human privacy and dignity, respect for private and family life
• rights of the child
• the data protection rights
• freedoms of thought, conscience and religion
• right to freedom of movement
• potential consequences to passengers' health, including possible harms from radiation
Right to privacy

According to the European Convention on Human Rights of 1950,

• Everyone has the right to respect for his private and family life, his home and his correspondence“ - Article 8 (1)

• There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others” - Article 8 (2)
Privacy

Applicability of ECHR Art. 8 (1):
• The European Court of Human Rights has given ECHR Article 8 a very broad interpretation.
• The concept of private life includes elements relating to a person's right to their image.
• The mere storing of data relating to the private life of an individual amounts to an interference.

Applicability of ECHR Art. 8 (2):
Given applicability of Article 8 (1), it is important to indicate:
• whether the interference is in accordance with the law.
• if the scans satisfy to the legitimate aim, proportionality and necessity principals.
“Scanned images of persons as if they were naked, equivalent to a virtual strip search” (EP, 2008)?

<table>
<thead>
<tr>
<th>Safeguards for privacy</th>
<th>Con arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>black and white silhouettes with blurred faces and other areas of the body</td>
<td>reveal very sensitive areas of private life and conditions, such as prostheses, breast implants, diapers, menstrual pads...</td>
</tr>
<tr>
<td>analysts are in separate rooms</td>
<td>abuses (for example, in Lagos airport)</td>
</tr>
<tr>
<td>analyst of the same gender (EU, UK)</td>
<td></td>
</tr>
<tr>
<td>alternative screening methods (USA, EU)</td>
<td>not all airports have capacity and staff</td>
</tr>
<tr>
<td>exemptions for the vulnerable groups</td>
<td>a concurrent risk that terrorists would then recruit children</td>
</tr>
<tr>
<td>the image would not be saved and would be destroyed</td>
<td>the breach of privacy is constituted by first the production and then the analysis of the image</td>
</tr>
<tr>
<td>the right to privacy can be considered as waived by the passengers since the travelers make agreements with airlines which include security requirements</td>
<td>not all such waivers are automatically effective (ECtHR case law: a waiver, to be successful, must be unequivocal and attended by minimum standards)</td>
</tr>
</tbody>
</table>
Do the scans add value in the war on terrorism and crime?

Pro arguments

• The governments claim that the use of the machines is justified and necessary in order to heighten security measures at airports and better protect the traveling public.

• They are considered to be more effective than metal detectors as they are capable of identifying both metallic and non-metallic objects, including plastic and liquid items.

• They are supposed to improve passenger flow. In contrast to manual searches requiring 2–3 minutes, the machines take only seconds to produce and interpret passenger data.

• Such an enhanced detection performance might also be achieved by a full physical hand search (so-called “pat-down“) or strip-search, but the use of scanners are thought to be quicker and less invasive.
Contra

- Cannot detect explosives carried inside the body.
- May not be able to distinguish foreign objects such as prosthetics and weapons. The percentage of false positives is high and it may increase the need for manual searches.
- An extremely finite period of time means evidence might be missed. Moreover, the operators may not have the required technical expertise to intercept the data.
(2)

- A price of a basic scanner: EUR 100 000 - 200 000 per item, excluding training, installation, and maintenance costs.
- The scanners are being implemented as a reaction to past situations. According to many security experts, such an approach will fail to anticipate the next bomber.
- Measures taken to address privacy concerns over the use of the scanners may dampen the machines' effectiveness in locating arms and explosives.
- While it can be acknowledged that there is a legitimate aim for the invasion of privacy, the effectiveness of scanners is questionable. Even if it is accepted that their use is necessary and proportionate, serious concerns about whether the intrusion is in accordance with the law still remain. Thus, it can be hardly stated that Article 8 (2) permits the limitation of privacy.
Right to data protection

The storage and retrieval of images

• The governmental agencies say the images cannot be stored, transferred, copied, or printed, and are permanently removed. BUT

• There is lack of complete, comprehensive and reliable information about what the devices actually are.

• The agencies need to retain the images as evidence, for testing and training purposes, or for later inspection to find out what went wrong with the scans if there were a successful terrorist attack.

• The TSA's Procurement Specs require that the machines have the ability to record and transmit images.

• According to a letter from 15 April 2010 from TSA to EPIC, the TSA possesses about 2000 body scanner photos from devices that the TSA said earlier “could not store or record images”.

• The experts also admit that the images are still being captured and stored by these “changed” devices.
Information to passengers

• The US S.A.F.E.R. A.I.R. Act: passengers shall be provided with (i) information about the images; (ii) information regarding the privacy protections; (iii) sufficiently detailed notice and an explanation of the alternative option for primary screening.

• The EU Commission proposes that appropriate, comprehensive and clear information on all aspects of scanner usage should be provided to the public at airports, before travelling.

• These proposals do not give sufficient details about how appropriate, comprehensive and clear information can be provided to the passengers in reality, before travelling and before purchasing the tickets, and who will be responsible for the information provision. This could at least enable the passengers to make an informed decision as to whether they wish to be scanned or not (if alternative methods are available) and/or whether or not to fly.
Excessive measure?

- If alternative and less intrusive screening methods are available, and if an individual is concerned about the implication of scans (due to disability, pregnancy, or other reasons) and consents to the alternative methods, then it may be considered excessive to require such a person to go through a scan.

*In summary*

it can be concluded that deployment of scanners cannot be currently regarded as in compliance with all the established data protection requirements and privacy standards.
Future?

Will new technologies determine the future in aviation security?

• One of the companies states that it is working on a system that would not require passengers to stop and stand still

• Flight Assistance Security Trolley

• Automatic Threat Recognition

• The X-ray transmission imaging technology can detect explosives carried internally

**BUT** over reliance on technology may have a negative effect

• technology can never be the “sole solution”, but only a means of reacting

• 100% security can never be achieved
The latest tendencies

• what is really needed is to change the system
• instead of reacting to past situations, there should be an intelligence-led system, with an element of randomness and unpredictability in security screening and the use of technology
• “behavioural analysis techniques”: it would then be at the discretion of the security staff to choose the appropriate screening techniques or technology
• “targeted passenger profiling” (although these techniques may raise separate human rights and equalities issues)
• with such an approach there may be no need to scan all passengers.
Alternative solutions?

- proposal to hand control of security back to the airlines
- proposal to train ordinary citizens how to stop terrorists on airplanes
- give up privacy at all
- refuse to fly whenever it is possible
Conclusion

• The use of both PNR systems and body scanners is increasing.
• While there are doubts about whether they add value to the war on terrorism and crime, it is quite obvious that these measures expose passengers to a significant loss of privacy and data protection rights.
• There appear many political and economic issues and policies, which greatly affect the security and privacy regime. It might be extremely difficult to find solutions, especially internationally.
• The point is that breaching people’s rights and freedoms can be justified under human rights legislation. But every security measure has to be clarified, justified and accompanied by strong and adequate safeguards.
• In the meantime the governments have failed to demonstrate that the measures are currently justifiable within the law. The proposed “safeguards” contain weak privacy provisions.
• Different organizations urge the governments to suspend the airport body scanner program until a comprehensive evaluation of the devices' effectiveness, health impacts, and privacy safeguards has been completed by an independent board of review.
THANK YOU

Comments? Questions?
olga.mironenko@jus.uio.no