SIAM

Security Impact Assessment Measures

Regime Interaction and Freedom Infringements

Centre for Technology and Society

Dr. Leon Hempel

Lars Ostermeier

Tobias Schaaf

Dagny Vedder

Deliverable D 4. 3

Case Study Report on Freedom Infringements (German Report)

Project number
261826

Call (part) identifier
FP7-Security-2010-1

Funding scheme
Collaborative Project

TABLE OF CONTENTS

1. Introduction

While the original empirical work of the project to date has focused on understanding the formal and informal factors at work in the evaluation and implementation of security measures at the case studies as well as future directions in security threats and technologies, SIAM now focuses on one of the issues at the core of the project, which is the impact of security measures upon civil liberties and human rights and, closely coupled to this, how these impacts can be mitigated.

Infringements can be understood broadly as the legal, social, or cultural norms that may be introduced upon by a security measure, while counter-infringement measures refer to technologies, rules, or procedures that reduce, mitigate, and minimize those intrusions. [1]

1.1 Objective

The case study sites are obligated to conduct workshops with stakeholders from the area of civil liberties, employee rights, politics, NGOs and watchdogs. The aim is to develop a catalogue of infringements, pre-emptive questions that could have prevented such infringements and finally counter-infringement measures that could mitigate the intrusion.

1.2 Workshop focus: Trust & Privacy Perspectives

The basis for SIAM is a model that encompasses as many perspectives as possible in a well-structured and easily understandable manner. On the highest aggregation level there are four fields: Privacy, Security, Efficiency and Trust. While SIAM already gathered respectable data for the dimensions Efficiency and Security the knowledge of the other two perspectives Trust and Privacy has to be enhanced. Therefore the conducted workshop focused on these two dimensions to supplement the data.

Trust

Trust encompasses the experience of the technology provider as well as of the technology scrutinized in using the technology. Beside the experience, the subjective perception defines in which way a technology achieves an appropriate acceptance level. Evaluation criteria for trust include for example the degree of discrimination regarding the use of technology as well as the potential physiological and psychological invasiveness of the technology (such as body scanner and claustrophobia).

Privacy

The privacy dimension of technology evaluation depicts the impact of a technology on the freedoms and rights of persons. Essentially data gathering and processing are major aspects of privacy

[1] Boyle, Phil. 2012. SIAM Workshop Guidelines

assessment. But also rights like intimacy and self determination are part of the privacy dimension and must be taken into account for an evaluation.

The complementary character of the workshop was in so far emphasized that the participants were asked to think in new categories and not to discuss already extensively debated issues.

In order to specify freedom infringements and possible counter infringement measures the results are sorted by the scope, normativity and intrusiveness dimension of SMTs. [2]

Scope

Scope refers to the spatial and temporal extent of the influence of a security measure upon a subject. Scope can have both physical and non-physical aspects. Physically, some security measures will be distinct in terms of both time and space. Physical barriers, gates, or fences, for example, are quite distinct on both space and time; they are physically identifiable structures that define borders between zones, and they cease to exert any influence over persons once they have been passed through. On the other hand, the use of surveillance cameras across city centres reflects a much higher degree of scope insofar as it may be difficult to physically remove oneself from the reach of this security. Scope also refers to how information gathered as part of the operation of a security measure is shared with others ('spatial' scope) or retained for future use ('temporal' scope). The long data is kept or the greater the numbers of individuals/agencies that have access to this data the greater the scope of the measure.

Normativity

Normativity describes the degree of compulsion associated with a particular measure/technology, or in other words how much agency an individual may exert over being monitored by a security measure/technology. Higher levels of compulsion to submit to a security measure/technology translate into means higher normativity, while lower levels of compulsion mean low normativity. An example of a highly normative security practice is airport mag-and-bag checks, which are highly compulsory and offer little room for passengers to exercise any agency. This security measure is highly normative, but it is worth noting that this normativity is loosening as many airports in Europe and North America move to institute 'trusted traveller' programs wherein frequent travellers with trusted profiles are rewarded with less stringent security measures while others are subject to greater scrutiny.

Intrusiveness

Intrusiveness refers to the kind and amount of damage a measure incurs for the subject. This includes direct physical contact or even penetration of the body to subjectively perceived infringement of social norms. In general, the less intrusive a security measure/technology is the less potential for infringement. However, this rule is subject to the provision that subjects must also be aware that they are subject to the security measure/technology. In other words, security measures cannot be so unintrusive that subjects are not aware they are subject to them; there should be no secret security measures.

[2] Boyle, Phil. 2012. SIAM Workshop Guidelines

1.3 Ethical Procedure and Workshop Participants

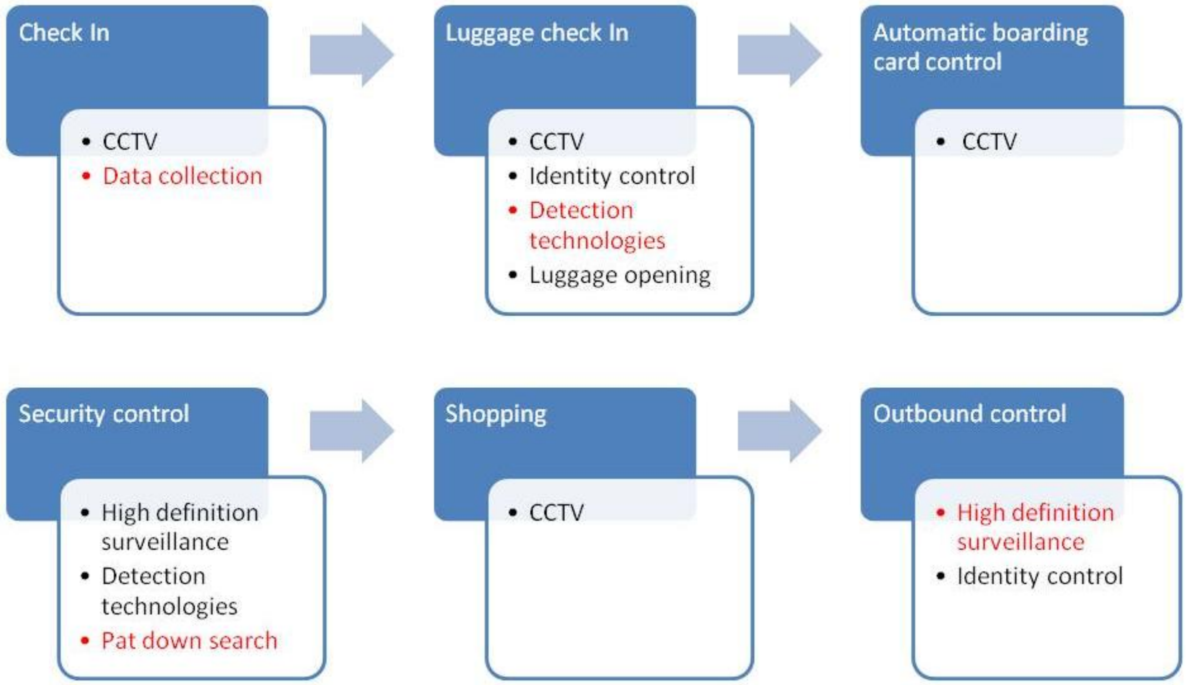
At the workshop experts from various respected fields participated. TUB was able to achieve the participation of representatives of a data protection agency, a passengers' rights agency, an airport employee union and an employee of a member of the German parliament. Due to the sensitivity of the topic TUB applied the 'Chatham-House-Rule' which guarantees anonymity for all participants but allows them to use gained knowledge as long as they do not reveal its origin. Furthermore, TUB gave out a letter of discreetness to all participants in which TUB states that all data will be anonymized and eventual recorded voice protocols will be deleted.

2. Workshop Procedure

TUB tried to answer the problem, that the participants, all respective experts in their field, may not have sufficient knowledge about processes at the airport environment. Therefore, TUB decided to set a focus on two key processes in which major technologies will have an interaction with whether the passenger or the employee. First TUB illustrated the passenger process from arriving at the airport until boarding the plane. Secondly, the path of the employee to his working space was reconstructed. The relevant technologies were depicted and sorted towards the phases in the processes. Afterwards, TUB chose certain technologies which were to be set focus upon to avoid redundant discussions.

2.1 The Passenger Process

Basis of the depicted passenger process was the travel story of a person who wants to fly to the United States of America. The USA was chosen to incorporate all steps of a travel procedure, which would not been the case if a travel arrangement within the Schengen area has been chosen.


Check In
- CCTV
- Data collection

Luggage check In
- CCTV
- Identity control
- Detection technologies
- Luggage opening

Automatic boarding card control
- CCTV

Security control
- High definition surveillance
- Detection technologies
- Pat down search

Shopping
- CCTV

Outbound control
- High definition surveillance
- Identity control

Chosen technologies and measures for discussions

- Data collecting at the check in

Those who book an air flight anywhere in the European Union will have to provide various data. These data will be processed, saved and in the case of a flight to the USA, shared with other states. These data contain more than only actual data about the passenger and the flight. It also contains data such as way of payment, meal wishes, past travel arrangements and upcoming ones. Since 2011 the EU and the USA agreed a treaty that allows sharing of the PNR. While within the EU the data is handled with a strict purpose and control by the DPA, the USA is saving the data for 15 years and is connecting the data with other sources of databases.

- Detection technologies for luggage

In the passenger process, the checked in luggage is separated from the owner and controlled by mostly automatic systems with different stages of detection technologies. If the first stage is not certain about the containment of explosives or drugs, the luggage will be send to another detection stage with different technologies. At the very end of such an automated process, the luggage will be opened and controlled by the respective security forces without the owner present.

- Pat down search

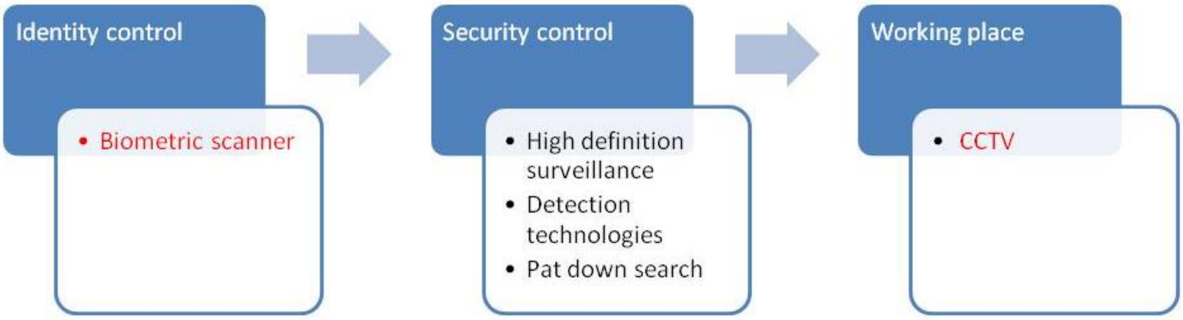
At the passenger control the controlled person must walk through a metal detector. If this detector sets an alarm the passenger becomes subject to a manual pat down search. A security officer will then use a hand metal detector to search the passenger manually with the so called 'hand-fallows-sensor' technique. This means that the control staff is obliged to touch the passenger with his hand along with the metal detector. He is also obliged to check the inside of the belt and the genitalia area.

- High definition camera surveillance

The federal police in Germany are responsible for the security checks of passengers at the airport. The federal police demands that the whole security check process is being monitored in the case of an incident. However due to new technological developments in hardware and software, the federal police began to implement high definition cameras. In a later stage and when software development is further advanced the HD cameras will be able to identify suspects automatically. So far this is not reliable enough for usage.

2.2 The Employee Process

To enable a discussion about the security technologies to which an employee is subject to, the path to the working station has been reconstructed.



Identity control
- Biometric scanner

Security control
- High definition surveillance
- Detection technologies
- Pat down search

Working place
- CCTV

Chosen technologies and measures for discussions

- Biometric identity control

The new Berlin Brandenburg International Airport is identifying its personnel with the hand vein scanner. Before an employee is allowed to enter the security controls to cross from land- to airside his identity will be checked. By scanning the hand vein with a sensor and comparing it with a template that is saved on his ID, the system is guaranteeing that the possessor of the ID is the legitimate owner of it.

- Closed circuit television (CCTV)

The airport is an area that needs constant video surveillance. This is guaranteed in Berlin with 1.800 cameras installed all over the airport premises. Some cameras are not recording all the time, but are recording if activated by a sensor (e.g. door alarm). All recorded material will be saved redundant on two different servers and can be monitored from the security control centre.

3. Surveillance Technologies

3.1 Freedom Infringements

The participants of the workshop discussed potential freedom infringements of surveillance technologies such as HD CCTV. On the one hand it was argued that the new capabilities like high density video recording – which gives the zoom feature a new quality – 360° dome cameras, and colour picture increase the potential infringements of personal rights regarding scope and invasiveness of CCTV operation. This affects e.g. the possibility of discrimination of the scrutinized people or even voyeurism through security personnel. The participants emphasized that these potential infringements are well-known, but have a much higher impact through new technological capabilities.

On the other hand the participants pointed out that the high quality resolution makes it possible to identify people and in consequence tracking of certain people becomes a realistic possibility. On the employee site this implies even the possibility to control their performance and behaviour during work without having a blind sport where no video surveillance is in operation.

It was argued by the discussants, that nowadays airports are perceived as zones with total security in place. Especially since 9/11/2001, security measures such as CCTV have strongly increased and through habituation the acceptance of such measures has increased too. However, in 2011 the constitutional court in Germany stated that airports – which are generally predominantly under public responsibility – are public spaces which mean that rights as freedom of assembly and freedom of expression are valid also in airports.[3]

3.2 Questions

During the workshop, the participants mainly raised questions concerning the specific usage rules of CCTV and the different degrees of surveillance depending on the security area.

- Which areas are under surveillance? Which degree of surveillance is necessary for which area? (incident vs. permanent)
- Are there any rules in place specifying the usage of CCTV?
- How is the access control managed?
- Which conditions are necessary for activating CCTV surveillance/ storage?
- What are the reasons for CCTV operation?
- Are there any signs informing the passenger or employee about CCTV operation?
- Which privacy-enhancing algorithms are available in order to ensure privacy?
- What kind of footage is necessary?
- Are there any blind spots?

[3] https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg11-018.html [accessed 07/17/12]

3.3 Counter Infringement Measures

One discussed counter infringement measure to reduce the scope of the possible impact on personal rights of passengers and employees by using surveillance technologies was to limit CCTV operation on certain incidents. Instead of using constant video surveillance in every security area, the participants argued to differentiate between security areas and their appropriate level of surveillance. All in all, they mentioned three different CCTV operation modes: no footage, live view and record.

Beside the different operation modes, the participants suggested individual user specific access levels to the data sources. Depending on the right to access, the user gets different representation of the footage (from statistical data to full access). Furthermore, all access regulations and user rights should be part of a common written data protection agreement in order to ensure accountability and transparency for employees. A similar code of conduct such as a house agreement which defined the legitimization of CCTV operation could be implemented for passengers.

In regard to normativity, the participants discussed solutions that try to cope with the constant surveillance conditions at the airport and lack of alternatives. If the passenger or employee has no freedom of choice, there must be at least a signage notifying that CCTV is in operation. Furthermore, the participants of the workshop stated to inform passenger and employees about the reasons and mode of operation.

In order to counter the intrusiveness aspects of surveillance technologies such as discrimination or control of performance and behaviour, the participants pointed out to use privacy-enhancing algorithms for video surveillance in order to blur faces or invert the video´s colour spectrum. Another discussed possibility in order to reduce the psychological impact of permanent performance control through video surveillance could be the provision of blind spots (e.g. restaurants, restrooms, waiting rooms) for employees.

3.4 Summary Table

	Infringements	Questions	Counter Infringement Measures
Scope	- Tracking of people (passengers and employees)	- Which areas are under surveillance? Which degree of surveillance is necessary for which area? (incident vs. permanent) - Are there any rules in place specifying the usage of CCTV? - How is the access control managed? - Which conditions are necessary for activating CCTV surveillance/ storage?	- Using only incident based video surveillance? - Access to the footage only if requested and in case of given reasons (accountability) - Provide different access levels (from statistical data to full access) - Data protection cooperate agreement/ House rule on CCTV operation
Normativity	- Being under constant surveillance – no alternative - Airport is not claimed as a free space any more (court decision)	- What are the reasons for CCTV operation? - Are there any signs informing the passenger or employee about CCTV operation?	- Usage of signage notifying CCTV operation - Inform passengers about the reason and mode of operation
Intrusivness	- Discrimination or even voyeurism by security personnel - Performance and behaviour control employees - Tracking of passengers and employees	- Which privacy-enhancing algorithms are available in order to ensure privacy? - What kind of footage is necessary? - Are there any blind spots?	- Usage of privacy-enhancing algorithms to blur faces or invert the video´s colour spectrum - Provide blind spots for employees

4. Detection Technologies

4.1 Freedom Infringements

When discussing about the security controls and the used detection technologies, the participants instantly started arguing about the body scanner which has been tested on the Hamburg International Airport. The body scanner was described as a perfect example of infringements but also counter infringement measurement. On the one side the body scanner reveals a highly controversial level of intimacy by being able to show every detail of the human body, but on the other side the technology that is not producing a picture can spare the controlled person the manual pat down control. The latter one has been depicted to be one of the most intrusive control measures there is. The rule hand follows sensor leads to touching of the body by control personnel. The procedure also entitles the touching of the inside of the belt and the genitalia area. This means that intimate areas of the body get physically touched. Both, the body scanner as well as the manual pat down is an invasive action and is likely to imply physical upset of the passenger.

Besides the physical intrusiveness, security controls do have a psychological impact. A false alarm rate of the metal detector leads other passengers to the conclusion that the passenger who caused the alarm might be suspicious. The same perception is valid for people who cannot use the normal control technologies, due to physical disabilities (e.g. pacemaker, artificial body parts etc.). The by standing passengers will think that this person has done something wrong. The persons are being stigmatized by being controlled manually or in another room.

Another possible infringement entails luggage getting lost. Remarkably in the travel terms and conditions it is normally agreed that luggage may be opened. The checked-in luggage will be opened without the presence of the owner and hand luggage in presence of the owner if there is an alarm. However, it has also been discussed that the property right is not being respected if belongings got thrown away because they are not allowed to be taken on the plane (e.g. Liquids, knifes etc.). In this connection it is noteworthy that one participant did not agree with this perception. He stated that people do know what is allowed and what is not to take on a plane and therefore have to take the consequences.

4.2 Questions

The following questions have been discussed during the workshop:

- Are the working conditions of the employees adequate?
- How high is the labor turnover rate?
- Do the employees receive frequently training?
    - In conflict management
    - In stress management
    - Technical training

- Are controls being clearly explained before passengers or employees arrive at the security checks?
    - Is it easy understandable?
    - Is it multilingual?
- Are passengers well informed about what happens to their checked in luggage?
- Is the distance of by standing passengers big enough to prevent overhearing or seeing the control process of another person?
- Is a clear allocation of the controlled passenger and his controlled belongings guaranteed?

4.3 Counter Infringement Measures

The workshop participants agreed that the security checks and their technologies are inevitable and that a certain level of intrusiveness cannot be avoided. However, a clearer and more transparent communication would help to increase the understanding of the measures. Since airports are a very international environment, a multilingual explanation of all the process that will happen whether with the checked in luggage or with the passenger himself should be provided. Especially, the manual control with the physical contact of the intimate area is of major importance and should be explained in details. In this context the false alarm rate of the metal detector and the fact which groups are not supposed to use the normal controls should be communicated as well to calm other passengers.

Furthermore, the control personnel are at the 'front line' and must be trained regularly not just in the technical area but also in conflict management. The workshop also agreed on the importance of employee motivation and that even in a multi-actor environment a common approach in that matter should be enforced. By providing long term job perspectives and incentives like higher salaries, the motivation and efficiency of control personnel will increase.

4.4 Summary Table

	Infringements	Questions	Counter Infringement Measures
Scope	• Being falsely under suspicion can cause a bad feeling which can last a very long time • Stigmatization	• Is the distance of by standing passengers big enough to prevent overhearing or seeing the control process of another person? • Is a clear allocation of the controlled passenger and his controlled belongings guaranteed?	• Increasing distance between controlled person and by standing persons
Normativity	• Security controls are inevitable	• Are controls being clearly explained before passengers or employees arrive at the security checks? • Is it easy understandable? • Is it multilingual? • Are passengers well informed about what happens to their checked in luggage?	• Easy accessible and multilingual information

5. Identification Technologies

5.1 Freedom Infringements

Regarding identification technologies the participants discussed possible freedom infringements of biometric identity control (vein, fingerprint, iris etc.) in order to get access to security relevant areas for passengers or employees at the airport. Examples for possible biometric applications are the German e-passport or ID cards for employees consisting of an RFID Chip that storage a biometric template of the person that has to be identified.

The participants of the workshop pointed out that there is a possibility of profiling if remote access on data is possible or unique RFID numbers are given. One participant stated that today it is possible to collect data from RFID chips having a minimum distance of 10 meters. Furthermore, the question was posed if airports would use tracking technologies in future if it is technical feasible.

Another possible freedom infringement, which was discussed during the workshop, is the spreading of biometric data for authentication purposes. One participant stated that there could be a danger building a central biometric data base that collects all passenger information. Furthermore, it was discussed that the passengers in general don´t know much about the data protection standards of every country, especially which data is stored und how data is processed. Most often it is not communicated who has access to the biometric data. In this case, the passenger as well as the employee, who uses the biometric systems, is losing the control over their own data.

If passengers or employees are forced to use biometric systems, trust concerns emerge. The participants of the workshop stated that the pressure to use a certain technology without providing an alternative technology is to be criticized. Beside the compulsion to use the technology, the participants emphasized also the aspect of psychological invasiveness. Missing information about the procedure and compulsory behavior are aspects that produce an inconvenient situation for the potential user during the identification process. One example, which has been mentioned are the newly introduced face recognition cabins, which are too narrow and not self-explanatory.

5.2 Questions

The questions that have been raised during the workshop concentrated primarily on the necessity of identification in order to indentify a person as well as on the usage of data. In the following, the raised questions are listed:

- Is the identification of a person necessary or is a verification process sufficient?
- Is the limitation of data use ensured?
- Is the specification of data purpose ensured?
- Is it possible for customers to access data storage?

    - Which information is accessible?
    - Is it easy to understand and to access the data?
- Is an external audit conducted?
- Are any alternative technologies provided to get access?
- Is a unique RFID necessary? Or is a random unique ID sufficient?
- Is the user used to the technology?
- Are any signs or explanations necessary in order to explain the procedure

5.3 Counter Infringement Measures

In order to prevent situation where biometric data is collected which is not necessary for the identification of a person, the workshop participants suggested the usage of active verification instead of passive identification. The verification process enables more transparency and control over biometric data and thereby has a positive impact on the scope of action of employees and passenger that have to use the technology. In comparison to the identification, the verification doesn´t need any personal data. The system only checks if the person (a certain kind of pattern) is identical with the person on the passport.

One possibility to ensure less degree of normativity, which was discussed in the workshop, is to provide technological alternatives. If this is not the case, the workshop participants suggested informing the people about the procedure, especially about the gathered data and processing. One participant emphasized that every passenger or employee should have the right for information access. This access should be as low as possible in order to guarantee transparency. Every institution that is involved in the identification process should follow a clear information policy.

One measure to counter the level of intrusiveness could be usage of a random unique ID on each request. From the perspective of the workshop participants this measure is the only way to avoid profiling of employees as well as for passengers while using RFID Chips on ID cards.

In general, the participants argued to involve an external data protection authority in order to ensure data protection, which is not effected by internal interests of certain actors. The monitoring should be conducted by a neutral institution, which is not dependent on the payment.

5.4 Summary Table

	Infringements	Questions	Counter Infringement Measures
Scope	• Creation of a unique profile • Enable access to biometric data – Spreading of biometric data	• Is the identification of a person necessary or is a verification process sufficient?	• Use verification instead of identification in order to allow access
Normativity	• Compulsion to use a certain technology • Risk of data abuse by external persons	• Is it possible for customers to access data storage? • Which information is accessible? • Is it easy to understand and to access the data? • Is the limitation of data use ensured? • Is the specification of data purpose ensured? • Are any alternative technologies provided to get access?	• Clear information police about data processing • Provide easy access to get information about gathered data • Provide technological alternatives for identification – Freedom of choosing
Intrusiveness	• Creation of a unique profile • Tracking of employees or passengers • Data protection influenced by economic interests • Inconvenient identification process	• Is a unique RFID necessary? Or is a random unique ID sufficient? • Is an external audit conducted? • Is the user used to the technology? • Are any signs or explanations necessary in order to explain the procedure	• Usage of random unique ID • Conduct external data protection audit • Signs or explanation how the identification technology has to be used

6. Information Processing and Communication Technologies

6.1 Freedom Infringements

In the discussion about information processing and communication technologies the workshop participants focused on the general problematic of the vast amount of data that is being collected and processed. In civil aviation regulation imposes a high level of normativity in that regard. Those who want to fly must accept that personal data is being collected and stored from various actors in the aviation complex. Airlines store booking data and are obliged to transfer certain data into the Passenger Name Record System (PNR). Access practices to the PNR vary from country to country and sometimes data is being shared between states. In general, legislation varies from state to state, which makes it impossible for passengers to understand all the processes or to keep track of their data. It is also the variety of actors, who collect data and store it, that raises the question about linked data that is not to be connected.

The actual scope of data collection and storage is therefore nearly impossible to depict, but can surely be imagined to be vast. This lacking transparency for passengers does have a psychological intrusiveness aspect. It is increasing insecurity for the passenger what is happening with all his personal data and makes him feel to lose control over it. One participant stated in that regard that passengers are not getting any information. They receive bits of it through the media which results in the conclusion that they don´t know what is happening to them if they travel.

6.2 Questions

The main infringements that were identified by the workshop experts are focused on the data collection, processing but especially on the eminent problem of control and transparency. Therefore, the pre-emptive questions that were developed to prevent or mitigate the problems are primarily about structuring the process.

- Who has which interests in which data?
- Which measures are actually relevant to provide a reasonable level of security?
- Is the specific technology necessary?
- Who has access to the data?
- How is the access to the data regulated?
- Is the storage of data really necessary?
- How is the data stored?
- How is a compliant practice ensured? Which mechanisms of control are in place?
- Who is in control of the data processes?
- What does the internal data protection officer say about the specific measures and processes?

6.3 Counter Infringement Measures

The discussants agreed upon that the scope of data can and must be reduced. It is not necessary to collect that many data to handle flight operations safe and secure. It must be clearly defined which data is required to handle on the one hand the flight business operations and on the other hand to handle the security problem in times of increase terroristic and transnational crime. It was also depicted that the access to the data must be more restricted, because not all data is adequate or needed for all actors. Thus a clear hierarchy of access shall be implemented and its compliance guaranteed. Another important aspect is the storage and deletion of data. Databases should have automated deletion cycles, which are not possible to be easily canceled. This means having mechanisms that prevent misuse or avoidance of the cycle e.g. by a single person.

In general all participants agreed that it is inevitable to collect data for the civil aviation processes and that most of the data is treated according to the legislation. The law imposes a high level of normativity for passengers and also for aviation actors. Without changes in the legislations it is rather problematic to mitigate it.

What can be mitigated, and this was stated to be the most important measure, is the level of intrusiveness. The feeling of loss of control by the passengers, but also by employees can be reduced by a high level of transparency and an increased control. Latter one is in Germany regulated by law that states that a company must have a data protection officer who is responsible for checking companies' policies on data protection. Here the participants pointed out that the officer must become more independent towards the management. So far the management appoints the data protection officer. One participant stated that he must have a stronger position within companies and must be independent. It often is a power game between the companies' departments. To enable the DPO one idea could be to make him member of the companies' board. The insufficient transparency in that area can be seen twofold. First the companies must give clear, accessible and easy understandable information to the passengers which data is being collected, why it is being collected, how it is being processed and how it is secured and deleted. The threshold for passengers to deal with that issue must be lowered to a level that rather encourages people to get involved in that topic. The second perspective is the legislative field towards companies. One discussant said that the various laws that influence data processing are confusing and sometimes just guidelines. He stated that a clear law is necessary and that 'A simple code of conduct is simple inefficient.'

6.4 Summary Table

	Infringements	Questions	Counter Infringement Measures
Scope	- Various actors collect data - Sharing of data - Danger of function creep - Centralized data collection	- Who has which interests in which data? - Which measures are actually relevant to provide a reasonable level of security? - Is the specific technology necessary? - Who has access to the data? - How is the access to the data regulated? - Is the storage of data really necessary? - How is the data stored?	- Reduction of amount of data that is being collected - Clear definition of purpose and restriction of usage accordingly - Access restriction - Automated deletion cycles
Normativity	- Legislations imposes data collection and storage		- Establish clear legal requirements and maybe reduce data collection
Intrusiveness	- Lack of transparency	- How is a compliant practice ensured? Which mechanisms of control are in place? - Who is in control of the data processes? - What does the internal data protection officer say about the specific measures and processes?	- Provide clear and easy accessible information for passengers and employees - Independent data protection officer