PRE-PRINT VERSION

The final version of this paper was published here:
Weydner-Volkmann, Sebastian (2017): "Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm." In: Elisa Orrù, Maria Grazia Porcedda, Sebastian Weydner-Volkmann (eds.): *Rethinking Surveillance and Control. Beyond the "Security vs. Privacy" Debate*. Nomos: Baden- Baden. 49-83.

Sebastian Weydner-Volkmann

Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm[1]

Introduction

Especially since the 9/11 attacks, travelling by airliner means to be subject to ever more intensive security procedures. In order to cope with screening for an increasingly diverse spectrum of threats, various actors in the aviation sector have promoted a shift in the paradigm of passenger screening. The International Air Transport Association (IATA), for example, suggested a 'Checkpoint of the Future' that more efficiently and less intrusively screens "different passengers in different ways" based on risk assessment procedures (IATA 2013: 8). As a broader industry initiative, it has since been redefined under the name "Smart Security" (IATA 2014). Furthermore, the US Transport Security Administration (TSA) has already introduced passenger differentiation and pre-screening programs, and in aviation security research, 'risk based screening' (RBS) has become a hot topic. While the term is often left unspecified, RBS is generally supposed to allow more targeted passenger screening using some form of 'predictive' risk data. It is hoped that this will allow a higher level of security, lower costs for the aviation industry and passengers, and less impact on the passengers – possibly all at the same time.

The main purpose of this paper is to describe the difference between the 'traditional' form of screening and the new paradigm of 'risk based (passenger) screening'. I propose to differentiate three main variants of RBS by means of the differences in the underlying risk analysis. As I show, even under a RBS paradigm, the security measures remain subject to various trade-offs and a conflict of interest between the provision of security, the

[1] Some of the ideas presented in this paper have been developed as part of the EU FP7 project XP-DITE. The main goal of XP-DITE is to develop a new, passenger centered approach to the design and evaluation of airport checkpoints that remains relevant even after a shift to risk based concepts. The paper is not meant to represent a shared view of the project consortium as a whole.

implied costs for the industry and passengers, and ethical, legal and societal implications.

In my paper, I use the terms ‘airport checkpoint (ACP) screening,’ ‘passenger security screening,’ and similar expression interchangeably to denote the screening of passengers and cabin bags for a defined set of ‘dangerous’ or ‘prohibited’ items. This definition of the scope of this paper means that I will not address various other types of screening practices that also happen to take place at airports, but that follow a different rationale, use different techniques and address different security concerns. For example, I will not address risk based concepts of checked baggage or cargo screening. In the same vein, practices of border control and customs checks will be out of scope for this paper. Such forms of screening may form part of future research.

My argument is structured into four main parts. In a first step, I briefly introduce the ‘traditional’ form of screening that is likely to be familiar for most people. In the second part, I then analyse what is actually new with regard to RBS. Drawing from Ulrich Beck, Herfried Münkler, Michel Foucault and other authors, I contextualize this change of paradigms in a wider cultural and historical development. This contextualization unveils some of the fundamental limitations and instabilities of risk management strategies, which also apply with regard to risk based approaches to passenger security screening. Based on this, I then briefly sketch out what different actors hope to achieve with an introduction of RBS concepts in the third part. In the fourth part, I then distinguish three variants of the RBS paradigm and expound the respective underlying assumptions with regard to the provision of protection against attackers. For each of the three variants, I also analyse the implications from an economic perspective and with regard to ethical, legal, and societal issues.[2]

[2] The identification of the relevant ethical, legal and societal aspects is based on a framework that includes a typology of ethical and societal issues of passenger screening which has been developed as part of the EU FP7 project XP-DITE (Volkmann 2013a, 2013b). In this paper I will not introduce this framework or the typology in detail in order to focus on the descriptive analysis of the RBS paradigm. The typology is based on similar efforts from other authors (Guelke 2011; Solove 2009), and identifies types of impact in three main categories: (1) privacy intrusion due to the revelatory function of passenger screening that I introduce in this paper, (2) the discrimination against vulnerable groups with regard to that intrusion (i.e. an unfair distribution of privacy intrusions), and (3) contributions to a broader development to restrict civil liberties such as the freedom of movement.

The traditional screening paradigm

In broad terms, passenger screening is a measure that is meant to make civil aviation more secure. While passenger screening cannot offer added protection against a range of attack vectors that have appeared over time (e.g. shooting down an airplane from the ground, hiding bombs in air cargo, pilot suicide), the security measure addresses the specific threat that *criminals amongst the passengers may attack the airplane*. Historically, especially two types of attacks proved to be relevant: (1) hijackings (including the use of the airplane itself as a weapon against other targets) and (2) bombings of airplanes (Kölle, Markarian & Tartar 2011: 93; Price & Forrest 2012: 41).

Types of items that are considered to substantially facilitate such attacks – mainly weapons (guns, knives, explosives) and certain tools – are compiled on a list of 'prohibited items', which then forms the basis of the passenger screening procedures (EU 2010: 16). Commonly, the effectiveness of the screening procedures is defined by their ability to prevent passengers from bringing such prohibited items on-board the airplane. Those procedures are conducted to a certain degree automatically via detection devices, but also manually by security personnel ('screeners') along a specified combination of steps. In this sense, airport passenger screening can be defined as a system of detection techniques that screen passengers for prohibited items.

In order to actually have any gain in the level of security, the screeners need to check whether a passenger has *hidden away* such an item *from plain view* – either on the body or in the luggage they carry along on the plane. In this sense, we can identify one function of ACP screening as revealing something that is not visible in plain view, i.e. kept private. This is why we can say that, to a certain degree, *all* ACP screening procedures will necessarily interfere with the privacy of *all* passengers that are being screened. Furthermore, ACP screening functions as a type of access control for aviation passengers (Traut et al. 2010: 14). Only passengers that are 'cleared' can enter the secure area of the airport and board the plane. The logic of ACP screening can, thus, be described by these two functions, the revelatory function and access control.

Currently, passengers and cabin bags (including jackets and other items that passengers bring along with them into the cabin of the plane) have to be screened separately (EU 2010: 12). Which items have to be 'divested' before the screening process is functionally dependent on the types of screening techniques applied. In order for a metal detector to work effectively for passenger screening, for example, all metallic items have to be divested and screened as cabin baggage.

For both passengers and cabin bags, two main steps can be differentiated in the process of security screening: primary screening on the one hand and secondary screening (or alarm resolution) on the other. In the traditional (and in the EU still current) paradigm of passenger screening, all passengers and all cabin bags are subject to the same primary screening procedures (Price & Forrest 2012: 258). Secondary screening, on the other hand, is only applied to a part of the passengers – either because of a random selection[3] or due to an alarm in primary screening. The reason for this differentiation into primary and secondary screening is the fact that some screening techniques, like a pat-down of a passenger, can detect very reliably whether or not a dangerous item is present; however, they require a lot of resources per passenger. Therefore, almost all airports in Europe conduct some less resource and time intensive form of primary screening: Instead of patting down all passenger, they make use of metal detectors and only use the more reliable but also more time consuming measures to resolve alarms and on a random basis.

For screening to be concluded, the regulation prescribes that all alarms need to be resolved so that the screeners can come to the satisfactory conclusion that no prohibited item is present (EU 2010: 12). In order to resolve those alarms, secondary screening can include more than one step and some steps may also be repeated. Furthermore, following the public outcry over the introduction of body scanners that produce an image of the body underneath the clothes (Deutscher Bundestag 2010; HIDE and RISE projects 2010; Zetter 2010), opt-out possibilities were introduced. Such steps of primary and subsequent secondary screening as well as opt-outs can schematically be expressed in a cascaded decision tree as shown in a simplified example for passenger screening in Figure 1.

[3] As opposed to the older regulation (EC 2002: 10), the current publicly accessible EU regulation (EC 2008; EU 2010) does not mention these random checks anymore. From personal experience as well as from what can be learned from the literature, however, we can assume that a part of the alarms sounded in primary screening are still random alarms. In any case, more detailed information on the percentage of passengers subject to random checks are classified due to the fact that, otherwise, it would be easier for attackers to calculate their chances to succeed in smuggling prohibited items through the screening process.

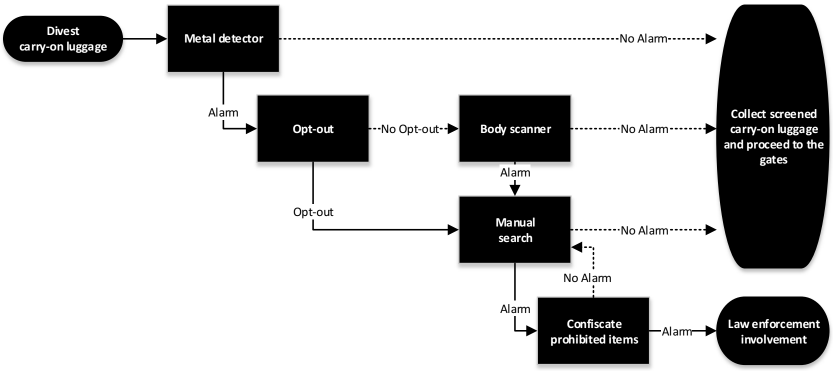

Figure 1: Simplified schematics of cascaded screening steps

Of course, it is *de facto* not always feasible to apply the same primary screening measure to all passengers alike. Persons with reduced mobility or with certain medical conditions, for example, may not be able to walk through a metal detector portal, and persons in a wheel chair would always cause an alarm making this detection measure useless. Consequently, checkpoints define alternative procedures for those passengers who cannot be feasibly screened using the standard procedure. These alternative procedures can be visualized schematically in a similar way. The complete system of screening measures can, thus, be conceptualized as different 'paths' through the checkpoint. On which path a passenger is screened depends on the occurrence of alarms and opt-outs during the process. While, in fact, passengers may in the end be screened in different ways, i.e. walk on different paths through the checkpoint, the schematic decision tree of the procedures is the same for all passengers (unless the procedures are infeasible, e.g. due to medical or mobility reasons).

Throughout the 1980s and 1990s, the organization of the screening procedures remained rather stable with walk through metal detectors and pat-downs as alarm resolution for passengers and single view x-ray screening and manual bag searches as alarm resolution for cabin bags. Already at the end of the 90s, however, several reports pointed at inadequacies of the procedures from a security perspective (Price & Forrest 2012: 224–226). As a reaction to the 9/11 attacks, then, international standards for screening were overhauled, new technologies were implemented and the process changed much more dynamically than before (Sweet 2004: 190). The situation that ensued has been characterized as a 'reactive approach' to screening (Kölle, Markarian & Tartar 2011: 40; 103), in which every attack triggers a reflex of almost hysterical activity resulting in the introduction of new security measures. In comparison to the situation of the 80s and 90s, this reactive approach changed considerably how the revelatory function is performed at airports. New technologies allow to screen for a much broader scope of 'prohibited items.' For example, newly introduced body scanners now allow to screen for non-metallic items during primary screening, and many airports have implemented explosives trace detection technologies for cabin bag and passenger screening.

This development has not changed, however, how the access control function works. It still functions as a binary exclusion of all persons who have not yet been screened for dangerous items and 'cleared' in the process. This is done by closing-off that part of the airport where passengers board the plane. In the aviation security literature, this closed-off zone is also called the 'sterile area' (Price & Forrest 2012: 228). Consequently, in the event that unscreened passengers enter this zone (sometimes called 'contamination'), all passengers that may have come into contact with them have to be screened again (Price & Forrest 2012: 233). By this spatial division, the passengers are strictly separated into two groups: cleared passengers and uncleared passengers. In the traditional screening paradigm, further differentiation is not necessary and not performed. The separation is done on the basis of the alarm/no-alarm-logic of the revelatory function, and screening data related to a cleared individual is not stored. The intended effect and the standard against which the traditional form of screening can be measured, then, is the complete exclusion from the sterile area of all passengers who may carry prohibited items with them. As an aviation security professional is quoted: "We are engaged in a complex game of cat-and-mouse and it is a truism to say that we must get it right 100% of the time whereas the terrorist only needs to get it right once" (Seidenstat 2009: 44).

In the face of a constant rise in the numbers of passengers each year,[4] this combination of a reactive expansion of the security measures and the goal of 100% exclusion of dangerous items proved to be highly problematic. As Klaus-Peter Siegloch, then Chairman of the German Aviation Association, said, passenger screening checkpoints have become the chokepoint of every airport (Spiegel Online 2011). Consequently, the regulators and the aviation industry have been looking for new ways to organize the screening procedures.

[4] For example, the number of airline passengers more than doubled since the 9/11-attacks: While in 2001, the number of airline passengers was estimated at 1.655 billion, this number rose to 3.441 billion in 2015 (The World Bank 2016).

From a theoretical perspective, especially the field of Surveillance Studies has addressed security measures at the airport relatively early (Adey 2004). The predominant approach in this field was to make use of Foucaultian concepts like the Panopticon. Consequently, in philosophy and the social sciences, passenger screening is often considered under the premise of being a form of surveillance (Zurawski 2015: 65, 86; Leese 2014a: 31–34, 50; Adey 2004: 501). If we look more closely at the second main function of airport screening, however, we have to raise the question whether this is in fact adequate. Rather than resembling the disciplinary mechanism of the Panopticon, of spatial parcellation and individualistic discipline (Foucault 1981: 251–255; Zurawski 2015: 28), the process of access control could be seen as being much closer to Foucault's 'juridical mechanism' of a binary logic of inclusion and exclusion (Foucault 2014: 19). Further evidence to support this can be seen in the terminology used by security professionals to describe this binary mechanism of inclusion and exclusion: Concepts like 'sterile area' or 'contamination' resemble one of Foucault's main examples for this binary mechanism, the plague, quite well. I will come back to this in the next section.

A new paradigm in passenger screening

In 2005/2006, the member states of the International Civil Aviation Organization (ICAO), which currently represents 191 states, agreed upon more stongly integrating risk assessment in their aviation security strategies (ICAO 2014: xi).[5] Within the EU bloc, the implementation of this agreement is part of the regulation labelled EC 300/2008. All measures of EU member states that exceed what is mandated by this common standard, the so called 'more stringent measures', are to be applied on the basis of risk assessments (EC 2008: Art. 6). Accordingly, it has been shown that specific member states such as Germany increasingly use conceptions of risk rather than the security/insecurity distinction when communicating publicly about civil aviation (Fischer & Masala 2011: 113–114).

This change can be seen in the context of a wider development, in which the members of the ICAO increasingly want to address the facts that they can never fully guarantee security against attacks and that the financial and

[5] The details of the standards and recommendations for the security concepts are classified, i.e. they cannot be discussed as part of this paper (ICAO 2014: 4–2).

human resources they are willing or able to spend are limited. In this context, risk assessment concepts are seen as a key to allow a more effective allocation of the limited resources (Poole 2009: 9). This means that in aviation, risk based approaches security are very closely connected to economic considerations: on the one hand regarding the *cost-effective allocation* of resources and, on the other, to limit the ever increasing cost for covering ever more threat scenarios in passenger screening by *redistributing* the available resources. In this sense, not only governmental actors see potential benefits (with regard to their role as provisioners of security against criminals), but economic actors from the aviation industry do so, too. Industry associations like IATA, for example, conduct concept studies to find out how a change towards risk based screening can limit the cost for increased security (IATA 2013, 2014). On a broader scope, it can be said that economic actors are quite open towards the adoption of risk based concepts (Poole 2009: 7–8). This is understandable once we realize that in most EU countries, while it is legally possible to finance the passenger screening efforts through national taxes (EC 2008: Art. 5), the security measures are financed directly (through ticket prices) or indirectly (through consumption at the airports) by the passengers (Poole 2009: 7). Consequently, the aviation industry, certainly has high stakes in finding ways to limit the cost for passenger screening.

This development towards an approach for airport screening that is to a wider extent based on risk assessment considerations is embedded in a more general cultural change. This context has been discussed extensively for some time, e.g. following the works of Ulich Beck (1986; also Giddens 1991). A common definition of ‘risk’ is that it contains three main aspects: (1) a conscious choice of action, i.e. a decision for one option against other possible; (2) the ‘negativity’ of possible outcomes of the options; and (3) the chances of realization of these outcomes (Rescher 1983: 6–7).

As Herfried Münkler (2010: 12–19) states, risk assessments always contain both a calculatory and a “playful” or “gambling-related” (*spielerisch*) element. Etymologically, ‘risk’ was coined in the economic context of long-distance trading by ship in the 14th century. Central to the economic conception of risk is that potential losses can always be compensated. Singular instances of risks with their various chances of realization can be *insured* or cleverly *put together* with other risks so that it becomes highly unlikely that the outcome proves ruinous for the trader. Münkler, therefore, concludes that for cultures of risk, the point of reference is not security as such, but rather *compensation* (Münkler 2010: 13). A certain ship may be lost at sea, but it can be assumed that other ships will safely reach their destination, and this can make up for the monetary losses or allow an insurance scheme. Risk strategies, therefore, are quite compatible with an economic perspective.

However, this playful approach to threats and dangers also plays an increasingly important role in contexts where compensation of losses seems implausible. This becomes clear when discussing 'aleatory' strategies and techniques of *governing* in more detail, for which Foucault has coined the label 'security dispositive'. As opposed to approaches that aim at the strict exclusion of the unwanted or at a meticulous form of individually internalized discipline, the security dispositive aims at seemingly more liberal forms of optimization and management of costs and benefits (Foucault 2014: 16; Gehring 2008: 155).

One of Foucault's examples for this is criminal punishment: While strict punishment and disciplination of undesired behaviour still play a significant role, cost-benefit analyses increasingly have an important influence, too. For example, the costs of criminal punishment are weighed against the costs of suffering from criminal behaviour, or the early release of convicted persons against the statistical likelihood of them becoming repeat offenders (Foucault 2014: 18–21). Foucault's argument here is that criminality is much more considered under the premise of traits specific to a given milieu. Those traits, so is the assumption, can be manipulated in such a way that it becomes possible to manage the occurrence of criminality in certain locations or in certain social strata. This type of strategy does not aim at a perfect separation of two groups, but rather at cost-effective interventions that maximize positive and minimize negative effects (Foucault 2014: 18; 37).

This also means that security dispositives do not relate to specific individuals but rather to a statistical mean of a given milieu, not to voluntary action but to potentialities of manifestation within a group (Foucault 2014: 38–39). On the one hand, this can mean that criminal punishment can be relented and freedoms be granted in some circumstances – for example, in case of a good prognosis, a convicted criminal may be released early. On the other hand, new surveillance and management techniques become necessary in order to collect the necessary data for the prognosis, to check whether this type of intervention is overall cost-effective and whether the prognoses are reliable. In order to render an uncertain future actionable, risk calculations, therefore, involve data collection about the past in order to predict various statistical means for a given milieu in an uncertain future. "'Risk' inherently contains the concept of control … It presumes decision-making. As soon as we speak in terms of 'risk', we are talking about calculating the incalculable, colonizing the future" (Beck 2002: 40).

If we follow Foucault in the assumption that security dispositives in the sense of aleatory governmental practices do not aim at individuals but at statistical means of a milieu, it becomes clear why negativities can be compensated: The success or failure of a governmental programme for the early release of convicted criminals on the basis of good prognoses is not determined with respect to one specific criminal, but with respect to systemic effects within specific groups. It may be acceptable if some of those who were released early become repeat offenders, so long as the underlying cost-benefit analysis holds true, i.e. so long as costs are saved and the large majority does not commit crimes again. For the success of such a programme and for the effectiveness of a risk calculus, the effects on a specifiable individual are irrelevant, so long as there are enough compensating cases. "Foucault suggests that instead of avoiding risks, security apparatuses embrace the concept of risk and profit from the emergence of advanced statistics" – not by making unwanted behaviour impossible, but by bringing it into connection with other phenomena that compensate potential, negative effects on a societal level (Leese 2014b: 501).

Of course, this kind of compensation seems to be rather unconvincing from the perspective of those who fall victim to one of the few repeat offenders. The reason for this is that in such cases, the playful element in the risk assessment seems completely out of place. Especially in the field of public security provision, the risk approach may therefore be deemed inadequate, since most of the time, we do not have the choice to withdraw from such a game. As Münkler says, the provision of public security in the form of the exclusion of violence in the pursuit of wealth and goods is the premise for the idea that risk assessments can work in such a 'playful' manner – which is why he assumes that cultures of risk always need to be embedded in worlds of security (Münkler 2010: 14–15). If this is not the case, we get mixed up in moral dilemmas that cannot be solved from within the logic of risk assessment, i.e. by pointing at costs and benefits. Accordingly, Münkler says that modern societies need to complement playful risk strategies with perfectionist security approaches, in order to create sustainable forms of security (Münkler 2010: 27). This highlights an important limitation and instability of risk based approaches in aviation security, as there is no real choice to withdraw from calculatory games that aim mainly at cost reduction.

With regard to the 9/11 attacks, however, another inadequacy of the risk approach becomes apparent that has previously been discussed mainly in the context of the environmental debates: the problem of 'uncontrollable risks'. People can always be dangerous to one another, and the possibility of the success of an attack can never be fully excluded. However, the potential 'negativities' can reach such an extent that they cannot be compensated even on a societal or global level. In aviation security, the stakes may be so high that the chances of failure cannot be justified from within the risk logic:

> "Specifically in aviation, screening policies necessarily must aim at minimizing Type II errors (false negatives), as an individual that was incorrectly assessed as harmless while being a potential offender poses the worst-case scenario and could cause devastating harm" (Leese 2014b: 496).

This brings a second important limitation and instability of RBS concepts to the foreground. In the light of potential catastrophic societal or global effects, the playful element again appears to be out of place. While it was possible to compensate the immense monetary loss due to the 9/11 attacks through governmental subsidies and credits (Sweet 2004: 12–15), this can hardly be said to be the case with respect to the loss of human lives, well-being as well as with respect to the direct political aftermath on a global level, namely the war in Afghanistan.

Despite such conceptual inadequacies, we can observe a trend in the field of public security provision towards more preventive risk based strategies in the EU and in many other states. "In post-9/11 security regimes, the efforts of policymakers to capture the future and fold it back into the present in order to render it actionable have reached new heights" – for example with regard to profiling measures discussed by the EU for the purpose of fighting terrorism (Leese 2014c: 497; 495). Thus, aleatory strategies are pursued in the fields of public security provision, even when they are not embedded in perfectionist forms of security provision and when losses cannot be compensated in any meaningful way. In such cases, risk strategies promise some form of control over the future that they in fact cannot guarantee:

> "'Uncontrollable risks' must be understood as not being linked to place, that is they are difficult to impute to a particular agent and can hardly be controlled on the level of the nation state. This then also means that the boundaries of private insurability dissolve, since such insurance is based on the fundamental potential for compensation of damages and on the possibility of estimating their probability by means of quantitative risk calculation. So the hidden central issue in world risk society is *how to feign control over the uncontrollable* – in politics, law, science, technology, economy and everyday life" (Beck 2002: 41).

While it can safely be assumed that this kind of aleatory approach to 'uncontrollable' risks is much more prevalent in 'risk societies' of what Beck calls the ‘second modernity’, it has been shown from a historical perspective that such forms of risk based policies have been developed at least as early as 1536 for the question of whether it is wise to lead a war against a neighbouring territory (Zwierlein 2012). This means that risk assessments have been transferred from economic contexts to the realm of governmental reasoning almost right from the start, even in cases where losses cannot be compensated through insurance schemes or accounted for in cost-benefit-analyses. This is the context in which we need to consider the current developments in aviation security regarding approaches to risk based passenger screening.

It is important to understand that the aforementioned limitations and instabilities at the core of risk management approaches do not *disqualify* them from being applied in the field of aviation security. Similar inadequacies can be identified for ‘perfectionist’ strategies of passenger screening, too, as we can never totally exclude the possibility of a catastrophic future. However, it is important to understand that risk based approaches, especially in the field of security provision, are not the one-stop rational solution to the problem of dealing with uncertain futures that they sometimes appear to be. Using risk approaches in contexts where compensation cannot be expected comes with a lot of conceptual contradictions and we should be careful not to uncritically believe in the promise of control they seem to give. It is therefore paramount to further analyse the specific benefits that are expected from RBS and how this new paradigm could be implemented in more detail.

Expected benefits of risk based passenger screening

As discussed above, traditional forms of passengers screening can be seen as *excluding* attacks from passengers on civil aviation by two basic functions: the revelatory function and access control. As I have mentioned above, however, the specific implementation of the two functions comes into conflict with other values (e.g. monetary costs or privacy intrusions). As I present in this section, one of the main promises of RBS is that it can deal with such ‘trade-offs’ in a rational manner.

In the debate on risk based screening concepts, three main areas play a prominent role for the assessment of the implications. Firstly, the *level of security* depends on how reliably the revelatory function performs, i.e. on how likely it is that prohibited items are found. At the same time, and secondly, more reliable screening techniques tend to have profound *economical implications* – costs go up and customer satisfaction goes down.[6] In addition to that, thirdly, the introduction of new or more intense screening measures tends to have *ethical, legal and societal implications*. For example, privacy questions have been at the core of a range of debates dealing with the introduction of the body scanners in Europe or the 'enhanced pat-down' rules in the US (Deutscher Bundestag 2010; HIDE and RISE projects 2010; Zetter 2010).

Risk based screening (RBS) is meant to address these trade-off situations, and some actors in the aviation sector hope that the trade-off trilemma between the level of security provision, costs, and ethical, legal and societal implications can be solved by it. At the core of RBS concepts is the idea to differentiate passengers into different risk groups and accordingly differentiate the intensity of screening, i.e. the amount of resources spent for the revelatory function.

With regard to the provision of security, it is hoped that risk assessments can complement the revelatory function of screening with a pro-active element. The hope is that this may help improving the likelihood of finding prohibited items even if they can currently hardly be detected during primary screening. Another argument for RBS is that it is paramount for a rational approach to screening to focus screening efforts on those passengers that are considered more likely to be attackers than others (Wagner 2014: 26–28). Critics of RBS, as we will see later on, however, are doubtful that passenger differentiation for screening will lead to an increased level of security and fear that it may, in fact, lead to adverse effects.

With regard to ethical, legal and societal aspects, it has been pointed out that focussing the intensity of screening efforts on some passengers may

[6] One of the major sources of revenue for airports is letting space in the building to duty-free shops and other businesses – especially in the 'sterile area'. Therefore, the footprint of a checkpoint is directly negatively related to the space that can be let to businesses. More reliable screening techniques like pat-downs or manual bag searches usually take more time per passenger. This means that in order to screen the same number of passengers per hour, more screeners and more space need to be allocated to the checkpoint – which means that the costs increase. Furthermore, since displeased persons tend to spend less money on consumption, 'passenger satisfaction' with the security screening measures has become another major cost consideration for airports. Pat-downs, manual bag searches and other reliable, but time intensive and more intrusive screening techniqes also tend to displease passengers more – which means that the amount of rent per square metre that airports can ask from the shop owners decreases.

have discriminatory or stigmatizing effects – e.g. with regard to Muslim passengers (Wagner 2014: 29; Georgi 2014: 18). Advantages, on the other hand, are seen in the idea that waiting times could be decreased and the procedures could be less intensive for the large majority, resulting in less inconvenience and less privacy intrusions (AEA 2014; IATA 2013).

From a cost perspective, a higher level of customer satisfaction for the large majority as well as less time and personnel intensive procedures have been named as expected positive effects, in addition to the ability to link simplified screening procedures with frequent flyer programmes (AEA 2014; Georgi 2014: 18; IATA 2013). The hope is that a shift in resources may limit the constant cost increase or even reduce costs (Wagner 2014: 30–31; Georgi 2014: 18). Of course, it is by no means necessary that the introduction of RBS decreases the costs for the aviation industry and the passengers. This depends on the ability to *shift* resources away from the majority of passengers, rather than just *add* extra measures for some passengers. It is interesting in this context, however, that (at least in the German public debate) the case for risk based screening is mainly made by economic actors (Wagner 2014: 30–31; Georgi 2014: 18).

Three types of risk based strategies for passenger screening

As discussed above, the proposal of a risk based approach to screening implies some kind of risk assessment as the basis for the design and implementation of differentiated passenger screening. However, what kind of risk analysis is proposed specifically, i.e. what the object of that risk analysis is, is hardly ever part of the debate (as an example see Wagner 2014). As will become clear in the following discussion, at least three main variants of the risk based screening paradigm should be differentiated in the debate on RBS, as they imply very different advantages and disadvantages for the three areas of implications discussed above (security, costs and ethics).

It is important to understand that these three variants are not mutually exclusive approaches. Instead, they should be understood as different kinds of strategies that can be (and in fact are) combined with each other. Even when they are combined, however, these strategies remain distinct from each other so that they can still be described as separate variants of the RBS paradigm.

Situational risk based screening

A first viable criterion for the distinction of the underlying risk analysis is the question whether the goal of the risk analysis is to classify *individual passengers* into different risk groups or to differentiate the use of screening resources based on *contextual factors*. The latter variant of RBS makes use of information that is not passenger related but based on broader information on the threat situation.

As an example of this, one could think of a situation in which a large amount of plastic explosives has been stolen. Compared with the threat situation before the theft, one could assume that there is the heightened risk for some airports in the country or region that attackers will try to smuggle some of this type of explosive on-board an airplane. A reaction to this assessment could be to intensify the search for corresponding explosive devices at those airports. Another example could be that *the flights* are differentiated into risk classes, e.g. based on the airline, the point of departure and the destination, the size or the maximum range of the airplane. This type of approach was proposed as part of the Dutch initiative SURE! (van de Wetering 2014). Based on such situational criteria regarding the flight or the threat situation, the passengers are then differentiated into different risk groups. Apart from the flight information, no other passenger-related information is necessary for the risk based differentiation, which means that any other passenger on the plane can be expected to have undergone the same form of cascaded screening procedures. I will call this variant of RBS 'situational risk based screening'.

In order to actually offer a higher level of security, there is a necessity for some form of data collection and analysis that allows a meaningful and adequate assessment of the threat situation. The increase in security provision that can be achieved by situational RBS is, thus, directly related to how well the threat situation can be assessed. If this can be done reliably and accurately, situational RBS can allow to adjust the screening procedures in a much more flexible way, depending on current situational risk assessment. Security-minded designers of airport passenger checkpoints are thus enabled to quickly implement new procedures.

From a cost perspective, on the other hand, situational RBS and a potential gain in flexibility may imply less reliability in the airports' or airlines' planning. Depending on how much flexibility is required on behalf of the checkpoint operators, differing screening procedures may require more personnel or lead to longer waiting times for passengers. Moreover, since many airports want to guarantee short waiting times for screening, it may be necessary to oversupply screening ressources to a higher degree. Airport operators cannot always assume that they are able to push the incurring costs for this type of flexibility towards the airlines and, consequently, to the passengers without further implications for their own business. Especially for smaller airports, this concern has been voiced in the past (UK Parliament 2012).

From an ethical and societal perspective, situational RBS does not seem to differ profoundly from the traditional screening paradigm at first glance. Exceptions to this may be more frequent changes regarding the screening procedures so that passengers may be less accustomed to the controls, especially if they may differ from flight to flight. On a broader perspective, however, one major concern could be the question whether it would really be politically feasible to *decrease* the intensity in the screening measures for specific flights or specific airports, even after a specific threat seems to have resolved. As we have seen above, the risk based approach to screening cannot provide a viable rational criterion for deciding that we can *take back or lower security measures* as long as there is still a certain chance, however minute, that they may prevent a catastrophic event.[7] Therefore, it remains unclear to what extent this variant of RBS can limit, stop or even reverse the steady increase in the interference with passengers' privacy and their freedom of movement (see also Volkmann 2014: 18–22).

Another reason for ethical concern with situational RBS is the distinct possibility that it may exacerbate potential discriminatory effects[8], even though passengers are differentiated according to non-personal, context-related information. In many legal contexts – like the EU – certain groups have been specifically recognized as vulnerable, such as groups identifiable

[7] As Birnbacher (1996: 201) writes, these kinds of questions refer us back to the field of ethics. According to him, the central question of 'risk ethics' is 'How safe is safe enough?'. On a metaethical level, the question then is how we can establish intersubjective validity when answering that question.

[8] Not only RBS concepts, but also traditional forms of screening may disproportionally affect some groups of passengers. Therefore, a specifiable group may be subject to a disproportionately more intrusive screening process. This could be the result of an accumulation of errors (e.g. false alarms) or of a different screening procedure for certain groups of passengers, either deliberately chosen (e.g. for passengers with reduced mobility) or inadvertently happened (e.g. resulting from an unforeseen inability to comply). Furthermore, the same screening procedure may differ in the level of intrusion for different groups of passengers (e.g. because a certain procedure is perceived as highly intrusive in a certain cultural or religious context).

by sex, gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, minority status, property, birth, disability, age or sexual orientation (EU 2010: C 83/396). In situational RBS, some of those groups (e.g. ethnic or social origin) may be affected disproportionally, as they may more frequently board planes that are considered high risk flights. It is not clear, however, which specific groups could be affected in this way. Currently, for example, high risk flight destinations may include the US or Israel which sometimes already have additional checks in place. Nonetheless, since all passengers on board those flights face the same procedures, including tourists and business travellers, it seems plausible that this risk of discriminatory effects may not or only tenably become manifest in many cases.

Passenger profiling using external risk data

Variants of RBS that do not use situational threat information but instead make use of information on the passengers can be further differentiated into two main approaches. On the one hand, there are efforts to allow the differentiation of passengers into risk groups based on *previously collected personal data* on the passengers. On the other hand, concepts have been proposed and implemented based on *behavioural data collected immediately before or during the screening process*.[9] In both variants, passengers are commonly separated into three risk groups which are then subject to procedures that differ with regard to the intensity and the resources applied. This can be seen with regard to the concept study 'Checkpoint of the Future' that was proposed by IATA: Three separate lanes are created to screen passengers according to their assigned risk category: 'enhanced' for passengers categorized into the higher risk group, 'known traveller' for passengers with the lower risk assigned (e.g. based on voluntarily submitted personal data), and 'normal' for all other passengers (IATA 2011).[10]

[9] As will become clear in the course of my argumentation, both variants have already been implemented by the Transport Security Administration (TSA) at many airports in the US.

[10] The different screening procedures for the three risk groups can be spatially separated into different screening lanes – as with the tunnels in IATA's concept study. This may not be the most cost effective method, however, since the application of

The main assumption behind passenger profiles-based RBS is that attackers are likely to be part of a specifiable group of passengers, that can either be effectively defined by intelligence services or statistical calculations (Adey 2004: 505–506). Correspondingly, the paradigm change is sometimes labelled with the slogan "Looking for dangerous persons, not (just) for dangerous objects" (Georgi 2014). In order to be able to select *some* specified passengers for more intensive screening measures, however, *all* passengers have to be identified to determine whether they should be selected or not. In this sense, the fundamental assumption in this type of RBS is also that it can make civil aviation more secure if the responsible authorities know the identity of the passengers (Soghoian 2009: 15). Although actors in the aviation security sector tend to avoid the word 'profiling',[11] I believe that it adequately describes the procedures that make use of already collected, checkpoint-external data on individual airline passengers. I will therefore call this type of differentiated screening procedure 'passenger profiling based screening.'

In current programmes in the US, the differentiation process is usually based on lists.[12] The risk analysis, thus, is not performed at the checkpoint

three levels of screening intensity can also be integrated in the same lane. The screening ressources are then applied dynamically when a passenger is identified and then categorized in one of the risk groups (IATA 2013: 19). As part of the programme SURE!, trials for a similar dynamic integration started in 2015 at Schiphol Airport (Ghee 2015). Passengers can then see only one type of lane, but additional screening procedures can be applied dynamically for some passengers without it being apparent to them.

[11] Especially in the US, but also in Europe, the word *profiling* is often seen in close relation to *racial profiling*, and thus avoided. With regard to RBS, there currently seems to be no nation-wide or Europe-wide programme for passenger profiling comparable to that of the US. In some national political debates, such programmes are rather seen with scepticism. In Germany, for example, the political discussion on this kind of differentiated passenger screening terminated quickly after opponents pointed towards the selection programmes (*Selektion*) in Nazi Germany. Prominent polititian Dieter Wiefelspütz, for example, said to the press: "Please cite me when I say: This is 'Selektion' at the airport – especially in Germany, we will have none of this" (*Schreiben Sie bitte ruhig: Das ist Selektion am Flughafen – gerade in Deutschland wird es das nicht geben*) (Weiland 2010; cf. also Georgi 2014: 18).

[12] Information on the criteria for putting someone on these lists or for assessing the likelihood that someone is an attacker have never been made publicly available. Furthermore, it is unclear to what degree this is an automated process (as it was

as such or by the authority responsible for screening. Instead, the TSA has the responsibility to establish the passengers' identities, to compare them to the respective lists, to then categorize the passengers appropriately into one of the three risk groups and to screen them accordingly. In addition to that, persons that have been put on the so-called 'no-fly-lists' are barred from entering the secure zone completely (Soghoian 2009: 15). With regard to the categorization of passengers, the US programme 'Pre' allows passengers to apply for less restrictive screening procedures. The relevant programme for the comparison of passengers with the selectee lists and the no-fly-lists, on the other hand, is called 'Secure Flight' (US TSA 2014a). These lists are comprised as an application oriented subset of the terrorist watch lists.[13] This means that the profiling itself is not performed by the

conceptualized for the programmes CAPPS I and II). Of course, it is highly problematic to use aleatory or statistical approaches in situations when there are extremely rare cases to provide the underlying statistical data (Press 2009). If it is true, however, that there is too little viable data with regard to aviation security for such statistical approaches, we have to ask the question whether the relevant authorities satisfy this statistical 'need for more cases' not so much by assessing the probability of an imminent attack directly, but by assessing the probability of someone belonging to a group that has been categorized as dangerous (e.g. 'religious extremists'). If that would be the case, it would exacerbate the lack of viable validation criteria, since the viability of the classification is based on further problematic presumptions – for example that we actually know which groups pose a threat to civil aviation.

[13] In general, we can probably safely say that the current practices of list compilations in the fight against terrorism are incompatible with fundamental democratic and human rights principles like the rule of law or the right to effective remedy – mostly due to the strict classification of nearly all details about these lists. This discussion however, is out of scope for this article, since the procedures for classification are not strictly part of the screening process. The no-fly-lists, for example, take effect *before* the screening process even starts as affected persons are usually not stopped and questioned by other authorities. This does not mean, however, that those lists are not used *at the airport* or even *at the checkpoint* in the search for suspected terrorists and that these practices would not raise severe issues. For example, from a rule of law perspective, it is hard to digest what happened to the Canadian and Syrian citizen Maher Arar: Due to inaccurate intelligence information, he was detained during a changeover of planes in New York without formal charges or access to a lawyer. Later on, he was brought to Syria against his will, where he was held for over 10 months in solitary confinement and was recurrently tortured. Subsequently, he was found innocent both by the Syrian government and in an official

TSA, but by another branch of the Department for Homeland Security.[14] Information on these lists is mostly confidential and, thus, quite sparse. By 2009, about 44.000 people are said to have been put on the no-fly-lists and about 75.000 people on the selectee lists (Soghoian 2009: 15). In addition to that, many of the known top terrorists are supposedly not even on these lists as the authorities fear that forwarding these names to other branches of the government may compromise intelligence activities (Kroft 2006; quoted from Soghoian 2009: 15). In 2007, Canada has established a similar programme under the name of 'Passenger Protect', which includes a form of no-fly-lists (Government of Canada 2014).

With regard to designing airport checkpoints, this implies the security requirement that for each of the passenger risk groups, adequate and reliable screening procedures are implemented. Therefore, the effective level of security that can be offered by the checkpoint is directly dependent on the reliability that attackers are classified by law enforcement agencies – and increasingly also by intelligence services – as high risk passengers. While it remains true that the level of protection against attacks on civil aviation is directly related to the detection probability of prohibited items, this probability is now also dependent on the risk classification of the passenger.[15]

Canadian investigation. He was set free and received an apology from the Canadian government (Soghoian 2009: 16–17).

[14] This division of labor, authority and responsibility makes it very hard to establish a more complete picture of the profiling activities. None of the decision criteria show up in the public documents on the TSA programmes Secure Flight und Pre. Furthermore, they are generally not subject to any publicly available scientific assessment (Bonß 2014: 8, 10). The TSA's 'privacy impact assessments' on these programmes – which are mandatory in the US – only refer to the data that is collected for the specific activity of 'list matching' (e.g. US DHS 2012: 6). As far as I could establish, the Office of Intelligence of the US Department for Homeland Security forms the relevant point of contact to the complex web of US intelligence services (Price & Forrest 2012: 147, 158).

[15] In the research literature, there is no consensus on whether this kind of passenger differentiation based on profiling could be undermined by a group of intelligent attackers, e.g. by testing which members of the group are classified as high risk and which are not. Depending on the specific implementation, it is also plausible that RBS may in fact *decrease* the level of security (Chakrabarti & Strauss 2002). In addition to that, some authors dispute the idea that it is mathematically feasible to use a form of *statistical* risk management in order to build profiles that help preventing *extremely rare* cases of attacks (Press 2009). Furthermore, it has been disputed that a checkpoint that makes use of the passenger profiling variant of RBS

In addition to that, in order to prevent attackers from being able to predict the procedures and adjust to them accordingly, it will remain necessary to randomly select passengers for additional screening measures – e.g. by moving them to a higher risk category.

As discussed before, applying passenger profiling at airport checkpoints makes it also necessary to identify all passengers at the checkpoint, so that they can be reliably classified in the 'correct' risk category. The level of security the checkpoint can offer is, thus, also dependent on how tamperproof the identification mechanism is – otherwise an attacker could spoof the identity of another passenger in order to be screened less intensely. However, such identification processes – e.g. via the passport – are notoriously unreliable. It is therefore hoped that biometric technologies allow increasing the protection against falsification of documents as well as the level of automation (Skillicorn 2008).[16] One problem with using biometrical passports for reliable identification is, however, that they are not mandatory in all countries. Thus, an attacker can currently still choose from a range of nationalities for a forged passport without biometric security. Furthermore, mandatory biometrics cannot help in the cases of state sponsored attacks, where attackers have access to 'legitimately' issued documents.

In their concept study, IATA considered the use of an iris scanner (IATA 2011), but another probable candidate for this would be fingerprint based biometrics. Passengers could have the necessary personal data stored in a shared database for more convenient identification processes. The possibility to make widespread use of biometric data that have already been stored for other purposes (e.g. for issuing biometric passports) would be highly problematic in the EU due to the current regulations on data protection.

From an economic perspective, differentiated passenger screening processes make it necessary to reliably predict how many passengers will be classified into which risk category at which times, so that the use of screening resources can be planned efficiently. Overall, it seems plausible,

can guarantee a higher level of security than traditional forms of screening at the same level of costs (Martonosi & Barnett 2006).

[16] When Bonß raises the question, how and according to which criteria biometric technologies are meant to allow a reliable differentiation between 'dangerous' and 'harmless' persons (Bonß 2014: 8), we can answer that this is not meant to be a function of biometrics in RBS at all. Biometrics, so it is hoped, allow a more reliable proof of identification so that an attacker cannot simply use an identity that is 'untainted' in order to be categorized as a low risk passenger.

however, that by making use of the profiling variant of RBS, airports can on average screen passengers more quickly and, thus, save costs and offer shorter waiting times to passengers (Lazar Babu, Batta & Lin 2006; Nie et al. 2009). Additionally, the profiling variant of RBS may allow the aviation industry to offer certain groups like frequent travelers access to less intensive screening procedures – provided the authorities offer some form of voluntary background checks and amend the lists accordingly.

From an ethical and societal perspective, the difference between profile based passenger differentiation and traditional screening concepts becomes especially apparent when the different risk categories are screened on separate lanes. More intensive screening for 'high risk passengers' requires that all passengers will be subject to some form of identification.[17] As discussed before, since passports and other travel documents are susceptible to forgery, this identification may involve biometric forms of identification. Depending on the details, biometric technologies can be implemented in a privacy respecting or in an intrusive manner. While biometric data is generally considered personal and sensitive and while such data even enjoys a higher level of legal protection (Petermann & Sauter 2002: 11), biometric information can be used both to *verify* passengers identity against an official identity token (e.g. the newer electronic passports), and to *identify* a passenger against a large database of previously collected fingerprints. In the former example, the biometric information can be processed in such a way that it is never stored outside of the tokens in the possession of the passenger, which limits the privacy impact and the potential for misuse of biometric data. In the latter example, on the other hand, the large scale collection and use of biometric data would raise severe ethical and legal concerns regarding questions of data protection, privacy and the potential for misuse by governments and criminals.

Apart from this potential issue regarding the use of biometric data, it seems plausible that a majority of the passengers may, indeed, be subject to less intensive screening measures. Thus, it may indeed be possible to limit the impact of *some* forms of privacy intrusions for them. It may be possible, for example, to reduce the rate of random secondary screening, which often involves more intrusive measures such as pat-downs by screeners and manual bag searches. This may be especially true for a smaller number of

[17] Depending on the specific procedures, this may be required for traditional forms of screening, as well. Since traditional screening procedures are not dependent on the passengers' identity, however, it is still (as of 2016) possible for some flights within Schengen area to board the airplane without showing any identification.

passengers categorized in the low risk group. At the same time, the majority of passengers, but again especially passengers in the low risk group, may also face much less restrictions in their freedom of movement.

On the other hand, this also means that at least some passengers are constantly subject to the more intensive and restrictive measures – which has already raised a number of questions regarding discriminatory effects (ACLU 2005). Furthermore, opaque decision and classification criteria may undermine the legal protection against discrimination (Leese 2014c). As has been discussed in the research literature, 'known traveler' programmes like 'Pre' may additionally reproduce socio-economic inequalities as they transfer differentiations and classifications from the private economy sector to the public security sector (Leese 2014b: 47).

Due to the necessary element of randomization, it will not be possible to guarantee that passengers will always be categorized in the same way. Depending on the level of transparency in the implementation, it is therefore also possible that a passenger may never be able to say for sure whether they have in fact been categorized in the higher risk category: Even when they are repeatedly subject to intensified screening procedures, this may simply be due to random selection. Since the relevant lists are highly confidential due to the sensitive nature of the information in them, this may make it impossible to explain to the affected passengers why they have been put on the lists and to offer an effective way to legally challenge such decisions – a fundamental requirement regarding the rule of law and for modern democracies in general. A case in point for this concern is the story of Rahinah Ibrahim, who was officially confirmed to have been put on the list by mistake. Despite the fact that the responsible agent testified to this error in court, she had to endure an undeniably Kafkaesque[18] eight-year legal process until she was officially notified that she was removed from the list (Boo Su-Lyn 2014).

> "US District Court Judge William Alsup also noted that the US government had placed Rahinah on its Terrorist Screening Database (TSDB) in October 2009 by using a 'secret exception' – which was deemed a state secret – to the reasonable

[18] Apart from the fact that the government tried to invoke national security exceptions to keep any procedural details regarding the lists confidential (including whether Rahinah was in fact still on these lists), she was at one point seemingly removed from the lists and allowed to fly abroad, only to find that she was put back on the list and was denied reentry into the US and, thus, was potentially without standing in the relevant court of justice (Boo Su-Lyn 2014).

> suspicion standard, defined as articulable facts that reasonably warrant the determination that an individual is engaged in terrorism.” (Boo Su-Lyn 2014)

In addition to that, there have been a number of cases in which passengers have been mistaken for suspected terrorists as their names matched or were very similar to one of a terrorist’s aliases (e.g. The Telegraph 2012). As a reaction to such cases, the TSA has created a ‘redress system’ for passengers who assume that this may be the case for them. In order to prevent the more intensive screening procedures, they can ‘voluntarily’ submit a range of documentation to establish their identity and receive a ‘redress number’ that they can submit for future travels (US TSA 2006: 9).[19] The Canadian ‘Passenger Protect’ programme has faced similar problems in the past (Humphreys 2013; The Globe and Mail 2014).

As discussed above, apart from the passengers’ identities, few personal data is collected and assessed in the screening process itself. Of course, this is due to the fact that during screening, only some form of list matching is performed, i.e. the collection and processing is done at an earlier stage someplace else. Since it is highly opaque what kind of data is used by whom and to what purpose and extent in order to assess which persons should be on such lists, the impact that is posed to passengers’ private lives is very hard to specify.

What is very clear however is the fact that the use of passenger profiling also creates a higher demand for mass surveillance activities. This is due to the fact that – as stated above – any *added security* and/or any reduction of costs *at the same guaranteed level of security* is directly dependent on the validity and completeness of these lists. This means that the protection against attacks from other passengers during the flight becomes directly dependent on the validity and completeness of intelligence gathering on any potential attacker of aviation security. The susceptibility of passenger screening to ‘false negatives’, i.e. the fact that missing something can always prove catastrophic, also holds true for the intelligence and law enforcement activities that produce these lists. By making the effectiveness of passenger screening at least in part directly dependent on the effectiveness of intelligence gathering, it is very likely that we also see a heightened demand for more surveillance activity at large. Since the sweeping surveillance activities have proven to rely also on the misuse of personal data, e.g. from electronic communications or non-public data from social media, we can conclude that the passenger profiling variant of RBS is likely to also

[19] Of course, it is highly problematic in itself to assume in such a situation that this information has been submitted ‘voluntarily’.

create a higher demand for highly sensitive and potentially illegally collected surveillance data on as many passengers as possible.

Behavioural analysis of passengers

Strategies of the third type of risk based screening, i.e. passenger differentiation techniques based on behavioural data collected immediately before or during the screening process, are based on the following psychological hypothesis: Attackers will unwittingly show certain behavioural peculiarities that can hardly be controlled by them. Trained security personnel can then engage in an interaction with each of the passengers and pay attention to these peculiarities. The fundamental idea behind this is that it is thus possible to detect 'bad intent' and use that as a basis for risk assessment (US DHS 2013: 2–4; US GAO 2013: 8; Weinberger 2010: 414). Similarly to the above mentioned slogan 'looking for bad people, not bad objects', this form of RBS is sometimes characterized as 'looking for bad intent' (Georgi 2014: 14).

One form of behavioural analysis based passenger differentiation – which has been implemented by the TSA as part of the 'Screening Passengers by Observation Techniques' (SPOT) programme – refers to a predefined set of 'behavioural cues' that are said to indicate elevated levels of stress, fear or the intention to deceive. From the flow of passengers, some are then selected for additional screening measures. Similarly, passengers can also be categorized as low risk ('managed inclusion'), when their behaviour is assessed accordingly. For the TSA's behavioural analysis activities, the SPOT process for detecting 'bad intent' has officially been described as follows:

> "BDOs [Behavioral Detection Officers] scan passengers in line and engage them in brief verbal exchanges while remaining mobile. BDOs identify passengers who exhibit clusters of behaviors indicative of stress, fear, or deception. BDOs identify passengers exhibiting behaviors that exceed SPOT point threshold for referral screening." (US GAO 2013: 10)

With regard to 'managed inclusion' the TSA writes the following:

> "TSA leverages a number of programs so that travelers may receive expedited screening when they travel. Passengers in [such] lanes generally move quicker compared to standard lanes, as those passengers leave their shoes, light outerwear, and belt on while keeping their laptop in its case and their 3-1-1 compliant liquids/gels bag. Managed Inclusion combines the use of multiple layers of security to indirectly conduct a real-time assessment of passengers at select airports." (US TSA 2014b)

As has been the case for the passenger profiling variant of RBS, the details on the specific criteria in these procedures – i.e. on the behavioural cues – are considered security sensitive and are therefore classified. However, the scientific basis for these programmes has been fundamentally put into question in the past, as the empirical evidence does not seem to support that such criteria are effective. Instead, some studies suggest that the probability of detecting deception is hardly higher than pure chance (Ormerod & Dando 2015; Weinberger 2010; US GAO 2013: I).

With regard to the high training and personnel costs for the behavioural detection officers, it is therefore unclear from an economic perspective whether this programme can be justified from a cost-benefit point of view. Consequently, the US Government Accountability Office has recommended to limit funding for the SPOT programme (US GAO 2013: I). With potential cost savings in mind, however, there are some efforts to develop automated behavioural analysis mechanisms with the use of sensors (Weinberger 2010: 415; Rogers 2014) – essentially, one could think of the use of automated lie detectors. The extent to which an automated analysis of behavioural cues may allow a more reliable detection of 'bad intent' remains unclear, however.[20]

At the current stage, problems of added costs can at least to a certain degree be compensated by measures such as managed inclusion, where some passengers are screened less intensely. When a certain part of the passengers are screened using less resources, this can make up for the added costs of training, staff and more intensive screening measures. In addition to that, in situations where the risk groups are spatially separated (as it is the case in some TSA checkpoints), managed inclusion can help to ensure that the use of the lanes is well balanced. However, one has to understand that – since the effectiveness and reliability of the detection of attackers is unclear – behavioural analysis that makes use of managed inclusion ceases

[20] The fact that, even though several scientific studies have dismissed such techniques as ineffective, such programmes have reached operational status (i.e. are not in a trial phase) and are well financed is in itself an interesting object for research. One important factor in this context is certainly that authors in the security research sector can at times avoid a critical discussion of their claims by a wider scientific audience when they point towards a need to keep parts of their findings confidential. In a wider context, however, there also seems to be a problematic understanding of science at work, in which many people seem to uncritically believe that statistical algorithms and the knowledge of psychological or physiological processes give an epistemic power to initiated scientists that is not obtainable for a critally thinking public. It is fitting that Sascha Lobo labelled this situation as the 'hour of the security esotericists' (Lobo 2014).

to act as what the TSA calls an 'added layer of security' (US TSA 2014b, 2015). This interpretation of the SPOT programme as added security is to a certain degree also represented in the research literature (Seidenstat 2009: 9). The metaphor, however, ceases to adequately represent what is happening, since whenever an attacker is mistakenly included in the low risk category, it can in fact *decrease* the probability of detection of dangerous items by the checkpoint. In those cases, it would thus be more fitting to call behavioural analysis more neutrally a *modifying security measure* rather than an *added layer of security*.

Instead of relying on the interpretation of behavioural cues, a second approach to behavioural analysis is based on the idea that longer interactions, such as structured interviews, can more reliably reveal whether someone is trying to deceive the security staff. Such structured interviews have been used in Israel for some years now. Here, the interactions take between some minutes and several hours (Wagner 2014: 23). This form of behavioural analysis is based on the hypothesis that in order to maintain a lie, we have to spend more cognitive effort. As a result of this, the amount of detail given in the interviewee's answers will deviate, depending on whether he or she is trying to maintain a lie or telling the truth. For example this could be a curious lack of detail in lengthy statements when asked to elaborate on the claimed background of the trip. A publicly available study supports the hypothesis that this technique may indeed help to detect persons who are trying to deceive the interviewer (Ormerod & Dando 2015). From a security perspective, this form of behavioural analysis therefore seems to offer some genuine advantages.

What is problematic for this type of behavioural analysis from an economic perspective is of course that the costs of operation increase drastically depending on the length of the interactions. It, thus, increases the challenge for concepts like 'managed inclusion' to make up for these higher costs. Especially at bigger airports, where an enormous amount of passengers have to be screened at peak times as fast as possible, longer interactions create prohibitive delays, as has become clear in the public debate on this 'Israeli model' of screening in the US (USA Today 2010).

From an ethical, legal and societal point of view, it can be said that both types of the RBS that make use of behavioural analysis may have a positive impact on some privacy aspects prominent in passenger screening. Depending on the specifics of the risk categorization, it seems plausible that a majority of passengers may less often be subject to secondary screening procedures that have a high privacy impact such as pat-downs or manual bag searches. Since the behavioural cue approach does not seem to make use of background information on the passengers' private life, this form of privacy impact remains low, too. For the structured interview approach to behavioural analysis, however, this may be different. It is, however, highly dependent on the type of questions to be answered. What is clear is that, due to the longer interactions and the requirement to answer truthfully, the implementation of such a measure in an EU context would mean that passengers' freedom of movement would be further restricted.

From an ethical and societal perspective, furthermore, the behavioural cue model's reliance on decision criteria that are hard to assess objectively may exacerbate effects of a categorization based on conscious or unconscious prejudices. Experiences from the US show that even from within the ranks of the BDOs, some believe that it aggravated systematic discrimination. For example, the New York Times writes:

> "More than 30 federal officers […] say the operation has become a magnet for racial profiling […] 'They just pull aside anyone who they don't like the way they look – if they are black and have expensive clothes or jewellery, or if they are Hispanic,' said one white officer, who along with four others spoke with The New York Times on the condition of anonymity." (Schmidt & Lichtblau 2012)

Since the decision criteria are not only classified but since it is also very hard to assess whether they have been applied correctly by a BDO, it seems almost impossible for passengers to challenge such decisions. The opaqueness of the decision processes, thus, also leads to a lack of accountability, which means that the TSA's emphatic claim to the objectivity of the programme (US DHS 2013: 2) can hardly be challenged or proven – neither in general nor in specific cases.

Conclusion

The main purpose of this paper was to analyse and describe what changes from 'traditional' forms of screening are implied when actors promote concepts of 'risk based (passenger) screening'. My argument followed four main steps. In the first part, I argued that passenger screening performs two main functions in order to reach its goal of protection against hijacking and bombing attacks on airplanes by preventing passengers from bringing prohibited items on-board with them: the revelatory function and access control. In the traditional form of screening the two functions implicitly follow the idea of absolute exclusion of passengers that carry such items. The recent 'reactive mode' of adding ever more security measures whenever there has been a successful or unsuccessful attack on aviation security, however, is seen as unsustainable in the long term by many actors in the field of aviation security, due to the incurring costs and the heightened awareness of ethical, legal and societal concerns.

In the second part of the paper, I then presented what some actors perceive as a solution to the trade-off trilemma between security provision, costs, and ethical, legal and societal implications: a risk based approach to screening that is based on differentiating passengers according to some form of risk assessment. As I have outlined, this 'paradigm shift' can be seen in the context of a larger cultural development towards governmental strategies of risk management. In this discussion, it also became clear that such forms of risk assessments have their own instabilities and limitations, for example when dealing with 'uncontrollable risks' or in the field of 'security provision'. Since in such contexts, which are both relevant for aviation security, losses cannot be adequately compensated, decision problems cannot be solved rationally from within the risk logic of costs and benefits. This means that using risk approaches for passenger screening introduces conceptual contradictions that should warn us to not uncritically believe in the promise of control they seem to give. For a more detailed view on the various implications of risk based screening, it therefore proved paramount to further analyse the specific benefits that are expected from this paradigm shift and how they play out in different variants of RBS.

In the third part of the paper I then outlined the main lines of conflict for decision problems with regard to passenger security screening as a trade-off trilemma. I showed that actors in the field of aviation security hope to address this trilemma by means of using risk based approaches to differentiated passenger screening.

In the fourth part, I proposed a systematic differentiation between three main variants of the RBS paradigm based on differences in the underlying risk assessment and based on the different implications for the trilemma between security, cost and ethics. A first distinction was made between RBS concepts that differentiate groups of airline passengers according to *contextual data regarding the general threat situation* and those that differentiate according to data related to the passengers themselves. I called the former variant of RBS 'situational risk based screening'. A second distinction was then made between RBS variants that differentiate passengers according to *previously collected personal data* on passengers and those that differentiate according to *behavioural data collected immediately before or during the screening process*. I called the second variant 'profiling based passenger screening' and the third variant 'behavioural analysis based passenger screening.'

It was not my intention in this article to provide an extensive normative evaluation or answer the questions of whether the paradigm shift towards RBS is worth pursuing or should be avoided. I believe that this question can only be answered in a detailed and public assessment of the likely outcomes of a *specific* programme. I believe, however, that such an assessment will have to follow the areas of conflict outlined in this paper. And I also believe that it will then be necessary to make a choice regarding what is meant to be the fundamental goal in introducing risk based screening concepts. Do we want to provide more security, reduce costs, or do we want to reduce the ethical, legal and societal impact of airport passenger screening?

In order to provide a meaningful contribution to the public and political debate on the future of passenger screening, any evaluation of the positive and negative implications of RBS will need to take into account that risk strategies will not 'solve' this trilemma, but rather have a considerable impact on the relevant trade-offs between security, costs, and various ethical, legal and societal aspects such as privacy, the freedom of movement, discrimination, transparency, accountability, and a heightened demand for mass surveillance or personal data. I hope that I have made a contribution to this necessary debate by making clear that many of the severe problems that I have highlighted are not mere historical accidents, but are rooted in the very basis of the trade-offs implied to a considerable degree by the underlying risk analysis.

Bibliography

ACLU (2005): The Four Biggest Problems With the „Secure Flight" Airline Security Program. https://www.aclu.org/technology-and-liberty/four-biggest-problems-secure-flight-airline-security-program (10/03/2015).

Adey, P. (2004): Secured and Sorted Mobilities: Examples from the Airport. In: *Surveillance & Society*, 4 (1). 500–519.

AEA (2014): Ensuring Secure Aviation while minimizing the hassle for passengers. In: *Association of European Airlines (AEA)*. http://www.aea.be/component/attachments/attachments.html?id=93&task=view (03/02/2015).

Beck, U. (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Beck, U. (2002): The terrorist threat world risk society revisited. In: *Theory, Culture & Society* 19 (4). 39–55.

Birnbacher, D. (1996): Risiko und Sicherheit – philosophische Aspekte. In: Banse, G. (ed.) *Risikoforschung zwischen Disziplinarität und Interdisziplinarität: von der Illusion der Sicherheit zum Umgang mit Unsicherheit*. Berlin: Sigma. 193–210.

Bonß, W. (2014) Eine umstrittene Neubestimmung – Nach welchen Kriterien sollen Passagiere am Flughafen überprüft werden? In: Wagner, K.; Bonß, W. (eds.) *Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Flugverkehr*. München: Universitätsverlag Neubiberg. 7–12.

Boo Su-Lyn (2014): Malaysian victim of Kafka-esque action in US travel ban, court rules. http://www.themalaymailonline.com/malaysia/article/malaysian-victim-of-kafka-esque-action-in-us-travel-ban-court-rules (18/03/2015).

Chakrabarti, S.; Strauss, A. (2002): Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System. In: *First Monday* 7(10).

Deutscher Bundestag (2010): Petition 9109: Datenschutz – Keine Zulassung von Ganzkörper-Scannern. https://epetitionen.bundestag.de/petitionen/_2010/_01/_03/ Petition_9109.nc.html (09/03/2015).

EC (2002): Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security (EC 2320/2002).

EC (2008): Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (EC 300/2008).

EU (2010): Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security (EU 185/2010).

Fischer, S.; Masala, C. (2011): Wandelt sich so Sicherheitskultur? Versicherheitlichungsdynamiken und Sicherheitsmaßnahmen am Beispiel des zivilen Luftverkehrs. In: *Sicherheit und Frieden* 29 (2). 109–116.

Foucault, M. (1981): *Überwachen und Strafen: die Geburt des Gefängnisses*. Frankfurt am Main: Suhrkamp.

Foucault, M. (2014): Vorlesung 1. Sitzung vom 11. Januar 1978. In: Michel Foucault: *Sicherheit, Territorium, Bevölkerung: Vorlesungen am Collège de France 1977–1978*. Frankfurt am Main: Surkamp. 13–51.

Gehring, P. (2008): Vorlesungen zu Staat/Gouvernementalität. In: Kammler, C.; Parr, R.; Schneider, U. J. (eds.) *Foucault-Handbuch. Leben – Werk – Wirkung*. Stuttgart: J.B. Metzler. 149–158.

Georgi, C. (2014): Risikobasierte Passagierkontrolle – Looking for dangerous persons, not (just) for dangerous objects. In: Wagner, K.; Bonß, W. (eds.) *Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Flugverkehr*. München: Universitätsverlag Neubiberg. 13–19.

Ghee, R. (2015): Behind the scenes of the new Schiphol Security Experience. In: *Future Travel Experience*. http://www.futuretravelexperience.com/2015/04/behind-scenes-new-schiphol-security-experience/ (02/03/2016).

Giddens, A. (1991): *Modernity and Self-identity: Self and Society in the Late Modern Age*. Palo Alto: Stanford University Press.

Government of Canada (2014): Safeguarding Canadians with Passenger Protect. http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/index-eng.aspx (08/07/2015).

Guelke, J. (2011): DETECTER: Detection Technologies, Terrorism, Ethics and Human Rights. Quarterly Update on Technology 10 (D12.2.10). http://www.detecter.bham.ac.uk/documents.html (07/07/2015).

HIDE and RISE projects (2010): Whole Body Imaging at airport checkpoints: the ethical and policy context. Policy Report No 2010/01. http://www.cssc.eu/public/ ETHICS-OF-BODY-SCANNER-POLICY-REPORT.pdf (03/07/2015).

Humphreys, A. (2013): First man on Canada's no-fly list denied legal funding for court fight. In: *National Post.* http://news.nationalpost.com/news/canada/first-man-on-canadas-no-fly-list-denied-legal-funding-for-court-fight (08/07/2015).

IATA (2011): IATA - Photo Gallery - IATA's Checkpoint of the Future. http://training-www.iata.org/events/agm/2011/gallery/Pages/checkpoint-gallery.aspx (28/01/2015).

IATA (2013): Checkpoint of the Future. Executive Summary. IATA. http://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf (17/12/2014).

IATA (2014): Smart Security. https://www.youtube.com/watch?v=GaPUNywU0oY&feature=youtube_gdata_player (19/03/2015).

ICAO (2014): Annex 17 to the Convention on International Civil Aviation. Security: Safeguarding international civil aviation against acts of unlawful interference. Montréal: International Civil Aviation Organization.

Kölle, R.; Markarian, G.; Tartar, A. (2011): *Aviation Security Engineering: A Holistic Approach*. London: Artech House.

Kroft, S. (2006): Unlikely Terrorists On No Fly List. http://www.cbsnews.com/news/unlikely-terrorists-on-no-fly-list/2/ (02/06/2015).

Lazar Babu, V. L.; Batta, R.; Lin, L. (2006): Passenger grouping under constant threat probability in an airport security system. In: *European Journal of Operational Research* 168. 633–644.

Leese, M. (2014a): *On security, once more. Assorted inquiries in aviation.* Dissertation zur Erlangung des Doktorgrades der Wirtschafts- und Sozialwissenschaftlichen Fakultät der Eberhard Karls Universität Tübingen. Tübingen: Eberhard Karls Universität Tübingen.

Leese, M. (2014b): Effektiv aber ungerecht? – Eine ethische Perspektive auf risikobasierte Sicherheitsstrukturen an Flughäfen. In: Wagner, K.; Bonß, W. (eds.) *Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Flugverkehr.* München: Universitätsverlag Neubiberg. 45–55.

Leese, M. (2014c): The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. In: *Security Dialogue* 45 (5). 494–511.

Lobo, S. (2014): Die Stunde der Sicherheitsesoteriker. http://www.spiegel.de/netzwelt/web/sascha-lobo-ueber-sicherheitsesoterik-und-staatliche-ueberwachung-a-945892.html (21/10/2014).

Martonosi, S. E.; Barnett, A. (2006): How Effective Is Security Screening of Airline Passengers? In: *Interfaces* 36 (6). 545–552.

Münkler, H. (2010): Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven. In: Münkler, H.; Bohlender, M.; Meurer, S. (eds.) *Sicherheit und Risiko. Über den Umgang mit Gefahr im 20. Jahrhundert.* Bielefeld: Transcript. 11–34.

Nie, X.; Batta, R.; Drury, C. G; Lin, L. (2009): Passenger grouping with risk levels in an airport security system. In: *European Journal of Operational Research* 194. 574–584.

Ormerod, T. C.; Dando, C. J. (2015): Finding a needle in a haystack: Toward a psychologically informed method for aviation security screening. In: *Journal of Experimental Psychology: General* 144 (1). 76–84.

Petermann, T.; Sauter, A. (2002): Biometrische Identifikationssysteme. Sachstandsbericht, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB). http://www.itas.kit.edu/pub/v/2002/pesa02a.pdf (07/07/2015).

Poole, R. (2009): The case for risk-based aviation security policy. In: *World Customs Journal* 3 (2). 3–16.

Press, W. (2009): Strong profiling is not mathematically optimal for discovering rare malfeasors. In: *Proceedings of the National Acadamy of Sciences of the United States of America* 106 (6). 1716–1719.

Price, J.; Forrest, J. (2012): *Practical Aviation Security: Predicting and Preventing Future Threats*. Oxford: Butterworth-Heinemann.

Rescher, N. (1983): *Risk. A Philosophical Introduction to the Theory of Risk Evaluation and Management.* Washington: University Press of America.

Rogers, C. (2014): A Slow March Towards Thought Crime: How the Department of Homeland Security FAST Program Violates the Fourth Amendment. In: *American University Law Review* 337 (2). 337–384.

Schmidt, M. S.; Lichtblau, E. (2012): Racial Profiling at Boston Airport, Officials Say. http://www.nytimes.com/2012/08/12/us/racial-profiling-at-boston-airport-officials-say.html (10/03/2015).

Seidenstat, P. (2009): *Protecting Airline Passengers in the Age of Terrorism.* Santa Barbara: ABC-CLIO.

Skillicorn, D. (2008): What are no-fly lists for? https://skillicorn.wordpress.com/2008/03/14/what-are-no-fly-lists-for/ (09/03/2015).

Soghoian, C. (2009): Insecure Flight: Broken Boarding Passes and Ineffective Terrorist Watch Lists. In: Seidenstat, P.; Splane, F. X. (eds.) *Protecting airline passengers in the age of terrorism*. Santa Barbara: Praeger Security International. 15–32.

Solove, D. J. (2009): *Understanding privacy*. Cambridge, Mass.: Harvard Univ. Press.

Spiegel Online (2011): Flugsicherheit: Nacktscanner versagen im Praxistest. http://www.spiegel.de/reise/aktuell/flugsicherheit-nacktscanner-versagen-im-praxis-test-a-783550.html (03/08/2015).

Sweet, K. M. (2004): *Aviation and airport security: terrorism and safety concerns*. Upper Saddle River, N.J: Pearson/Prentice Hall.

The Globe and Mail (2014): The problems with Canada's no-fly list. http://www.theglobeandmail.com/globe-debate/editorials/the-problems-with-canadas-no-fly-list/article20284034/ (08/07/2015).

The Telegraph (2012): Airline pulls 18 month old girl off plane in 'no-fly' alert. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9259324/Airline-pulls-18-month-old-girl-off-plane-in-no-fly-alert.html (18/03/2015).

The World Bank (2016): Air transport, passengers carried. International Civil Aviation Organization, Civil Aviation Statistics of the World and ICAO staff estimates. http://data.worldbank.org/indicator/IS.AIR.PSGR (21/07/2016).

Traut, A.; Nagenborg, M.; Rampp, B.; Ammicht Quinn, R. (2010): Körperscanner – Sicherheiten und Unsicherheiten. In: *Forum Kriminalprävention* 1. 14–20.

UK Parliament (2012): Civil Aviation Bill - Memorandum submitted by the Manchester Airports Group (MAG) (CA 05). http://www.publications.parliament .uk/pa/cm201212/cmpublic/civilaviation/memo/ca05.htm (28/01/2015).

USA Today (2010): Our view on airport screening: Why Israel's air security model wouldn't work in the USA. http://usatoday30.usatoday.com/news/opinion/ editorials/2010-12-22-editorial22_ST_N.htm.

US DHS (2012): Privacy Impact Assessment Update for Secure Flight. April 13, 2012. TSA/Secure Flight Nr. DHS/TSA/PIA-018(e). Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf (03/10/2015).

US DHS (2013): Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted). Office of Inspector General Nr. OIG-13-91. Department of Homeland Security. http://www.oig.dhs.gov/assets/Mgmt/2013/ OIG_13-91_May13.pdf (03/10/2015).

US GAO (2013): TSA Should Limit Future Funding for Behavior Detection Activities. United States Government Accountability Office. http://www.gao.gov/ assets/660/658923.pdf (09/02/2015).

US TSA (2006): Privacy Impact Asessment for the TSA Traveler Identity Verification Program. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/ privacy/privacy_pia_tsa_otsr.pdf (03/10/2015).

US TSA (2014a): Frequently Asked Questions - Secure Flight. http://www.tsa.gov/ content/frequently-asked-questions-secure-flight (10/03/2015).

US TSA (2014b): What is Managed Inclusion? http://www.tsa.gov/traveler-information/what-managed-inclusion (10/03/2015).

US TSA (2015): Layers of Security. http://www.tsa.gov/about-tsa/layers-security (10/03/2015).

van de Wetering, E. (2014): *A Risk-Based Passenger Screening Security Architecture optimized against adaptive threats. MA-Thesis Erasmus Universiteid Rotterdam.* http://thesis.eur.nl/pub/16046/Scriptie-Econometrie-2014-Elbert-van-de-Wetering-publieke-versie2.pdf (03/10/2015).

Volkmann, S. (2013a): XP-DITE Deliverable D7.1: Ethical and legal requirements for system design.

Volkmann, S. (2013b): XP-DITE Deliverable D7.3: Methods for assessment and quantification of compliance with the given ethical requirements.

Volkmann, S. (2014): Angewandte Ethik für öffentliche Sicherheit: Versuch der Bestimmung einer Bereichsethik. In: Riescher, G.; Gander, H-H. (eds.) *Sicherheit und offene Gesellschaft. Herausforderungen, Methoden und Praxis einer gesellschaftspolitischen Sicherheitsforschung. Bearbeitet von Sebastian Volkmann und Stefan Weidemann*. Baden-Baden: Nomos. 13–41.

Wagner, K. (2014): Vom Werkzeug zum Täter – ein Paradigmenwechsel im zivilen Luftverkehr? In: Wagner, K.; Bonß, W. (eds.) *Risikobasiert versus One Size Fits All. Neue Konzepte der Passagierüberprüfung im Flugverkehr*. München: Universitätsverlag Neubiberg. 21–33.

Weiland, S. (2010): Flughafenkontrollen: Plan für Passagierselektion empört Politiker. http://www.spiegel.de/politik/deutschland/flughafenkontrollen-plan-fuer-passagier-selektion-empoert-politiker-a-736850.html (10/03/2015).

Weinberger, S. (2010): Airport security: Intent to deceive? In: *Nature News* 465 (7297). 412–415.

Zetter, K. (2010): National Opt-Out Day Called Against Invasive Body Scanners. https://www.wired.com/2010/11/national-opt-out/ (21/07/2016).

Zurawski, N. (2015): *Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung*. Berlin: Forschungsforum Öffentliche Sicherheit.

Zwierlein, C. (2012): Grenzen der Versicherbarkeit als Epochenindikatoren? Von der europäischen Sattelzeit zur Globalisierung des 19. Jahrhunderts. In: *Geschichte und Gesellschaft* 38 (3). 423–452.