EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

INTERNATIONALES ZENTRUM FÜR
ETHIK IN DEN WISSENSCHAFTEN (IZEW)

How Smart Is "Smart Security"? Exploring Data Subjectivity and Resistance

Final Report. Published in November 2015.

Main Authors:
Andreas Baur-Ahrens
Marco Krüger

Contributing Authors:
Regina Ammicht Quinn
Matthias Leese
Tobias Matzner

MEDIADEMOCRACYFUND

FORD FOUNDATION

OPEN SOCIETY FOUNDATIONS

Recommended citation for this report:
Baur-Ahrens A, Krüger M, Ammicht Quinn R, Leese M and Matzner T (2015) *How Smart Is "Smart Security"? Exploring Data Subjectivity and Resistance*. Final Report. Tübingen: IZEW. Available at: http://hdl.handle.net/10900/66898

doi:10.15496/publikation-8318

Disclaimer

The International Centre for Ethics in Sciences and Humanities (IZEW) at the University of Tübingen, Germany, retain all rights, including intellectual property rights, in and to final works resulting from this project.

The IZEW fully complies with the license section as agreed upon in section VIII. of the *New Venture Fund Grant Agreement*. The final report will be accessible on the website of the centre, once it is approved by the New Venture Fund, the Media Democracy Fund, the Ford Foundation and the Open Society Foundations.

All activities by University of Tübingen, were and are consistent under the Internal Revenue Code Sections 501(c)(3) and 509(a)(1), (2) or (3). If any lobbying was conducted by University of Tübingen, (whether or not discussed in this report), University of Tübingen, complied with the applicable limits of Internal Revenue Code Sections 501(c)(3) and/or 501(h) and 4911. University of Tübingen, warrants that it is in full compliance with its Grant Agreement with the New Venture Fund, dated June 11, 2015, and that, if the grant was subject to any restrictions, all such restrictions were observed.

This report is the result of a research project which was conducted by a team of researchers from the University of Tübingen in the time from June to September 2015. The project was funded by the Media Democracy Fund, the Ford Foundation and the Open Society Foundations within the framework of the "Quantified Society Grants" under grant agreement no. 06112015.

Executive Summary

Currently, aviation industry associations promote smart security initiatives as a means aiming at increasing the level of security, while at the same time being cost efficient and improving the travel experience of passengers. This tempting promise is to be fulfilled through the implementation of data-driven security routines. Smart security means the use of individually tailored risk assessments in order to allocate a particular passenger to a pre-defined risk category. The interplay of an assemblage of security routines underpinned by data form the core of smart security. Using passengers' data from a range of sources, however, "smart security" turns out to be a challenge to existing human rights standards in general and to passengers' privacy in particular.

This report identifies human rights implications which the introduction of smart security initiatives at airports might entail. Although the introduction of smart security is in an early stage, some test projects at airports like Amsterdam Schiphol (the Netherlands) or London Heathrow (UK) are already running. Proponents of smart security are also active on the political level through lobbyism for the introduction of voluntary known traveller programmes. An example is the "Registered Traveller Programme" (as part of the EU's "Smart Borders" project. Particularly as smart security is not yet comprehensively introduced, it is the right time to consider and analyse potential human rights problems connected to a broader implementation of smart security routines.

The case study at hand reviews the existing academic literature and summarises the state of the art in the field of data-driven profiling as fundament for its empirical research. During the research, eight interviews with actors from different backgrounds, including representatives of aviation associations, state authorities and the civil society have been conducted. The interviews reveal both the current development in smart security and the human rights implications of this new security paradigm. The interviews are supplemented with an analysis of policy documents from aviation associations.

Core Findings:

Smart security does not necessarily contribute to a higher security level at airports. More fundamentally, the need for more security cannot just be stated but has to be discussed within the civil society. Risk-based passenger screenings are working through differentiation which inherently contains either positive or negative discrimination. Data-driven predictions must not be seen as objective knowledge but as results of a probabilistic process.

Smart security might be suited to enhance the passenger throughput at airports and, hence, increase the cost efficiency for profit-oriented actors like airports and airlines. This cost efficiency, however, is likely to result in other costs: privacy and human rights of the passengers including discrimination. Security seems not to be the primary motivation to introduce smart security compared to economic aims.

In a dynamic data-driven security environment, static human rights safeguards such as the EU Charta on Fundamental Rights become ineffective, because of their incapability to adapt to ever-changing data sources. Even if smart security initiatives are less intrusive on a physical level, they are the more intrusive in terms of privacy and human rights issues.

Bearing in mind the human rights implications of smart security, the report identifies six central policy gaps and issues recommendations to address them.

1. Why and how should smart security routines be implemented?

The need for a higher level of security has to be proven before introducing new security devices and/or methods. Considering economic factors like cost efficiency, randomly adjusted intensities for security controls seem to be preferable to opaque data-driven routines due to privacy considerations, possible discrimination and misuse of information.

2. What is lobbyism for smart security aiming at?

European as well as national authorities should be aware of lobby strategies of the aviation industry. Known traveller programmes might initiate a mind shift towards an increased acceptance of data-driven profiling. However, public acceptance is not to be confused with ethical acceptability. Thus, human rights issues in general and privacy issues in particular need to be thoroughly reflected and protected before permitting data-driven profiling.

3. What data sources should (not) be used for smart security and how are passengers to be allocated to pre-defined categories?

It has to be ensured that sensitive passenger data are not in the focus of data collection. Voluntarily given data must only be used with regard to the purpose of their collection. Proponents of data-driven profiling must provide a convincing argumentation on a) how risk categories increase the overall level of security while avoiding any discrimination of passengers; and b) why personal risk assessment is an advantage in terms of security compared to non-discriminatory, standardised security screenings.

4. What measures are undertaken to counter the misuse of data?

European and national regulators need to make sure that privacy issues are considered in aviation security. A convincing privacy concept that entails effective safeguards should thus be a precondition for further negotiations on the introduction of data-driven security routines.

5. Who is accountable for security decisions in the end?

A clear-cut concept of accountability ought to be a criterion for the introduction of smart security routines. Prior to the implementation of data-driven routines, it needs to be examined how human rights safeguards are to be altered in order to provide an effective human rights protection.

6. How could appeals against security decisions be part of smart security?

The possibility to challenge security decisions is crucial in terms of human rights standards. Regulatory bodies need to make sure that security decisions can be made transparent for the treatment of appeals. Overall, the involved actors are willing to implement appeal mechanisms. Thus, it is up to the regulators to design *appeals* procedures that ensure an independent appeal procedure that is subject to public supervision.

Smart security seems to be a project of the future. The ongoing discussion of known traveller programmes, however, is a matter of the present and a vital element for causing a mind shift towards an unproblematised use of data-driven security routines. This report, thus, aims at sparking a public debate on how security needs to be shaped in order to ensure human rights rather than sacrificing them for the alleged sake of security.

Contents

1. Introduction

Imagine you want to fly from Amsterdam, Netherlands, to Rome, Italy. You enter the airport as you always do when you have business meetings abroad. You approach the security checkpoint, you put your belongings into the tray and walk through the body scanner. There is no operator examining the x-ray image of your luggage. It is examined in a central room, away from the noise of the checkpoint lane. The body scanner's software programme runs a certain security routine, as you are not unknown to the security authorities. You are not a criminal, of course. However, data-driven profiling affects everybody and consequently also predicts your risk score. Neither you nor the security personnel know your risk category, but you recognise that a pat-down does not seem to be necessary. You can take your hand baggage without interruption. Apparently, the officer in the central x-ray room found nothing suspicious. While you are heading to your gate, you are still wondering why your colleague behind you is denied access to the gate.

The notion of smart security has been on the rise for some time now. Security agencies are overwhelmed in their struggle to fight against terrorism, global criminal networks, human trafficking, contraband, or illegal migration by the sheer amount of individuals and goods on the move. In this complex situation Big Data has been called upon for the rescue. Smart security systems, so the argument goes, can help to structure and make sense of large amounts of data in order to render populations "transparent" and thus to identify possible security threats without interrupting flows of global mobility and connectivity. The recent revival of the Foucauldian concept of biopolitics as an analytical tool in security studies scholarship bears witness of this trend.

As Michel Foucault (2007; 2008) has demonstrated, mobility has become a prime target for political intervention at the threshold of modernity – and most notably for a contemporary politics of security that thrives on the very openness of our times. It is a security politics that embraces the data streams of our digitised world in order to calculate, estimate, and assess the risk that circulating elements possibly pose. Smart security today is an assemblage of different technologies that build on the promise of the algorithm – the promise that it would be possible to predict future harm through the analysis of data at scale, and thus to render it workable. In other words: to fold the future back into the present, where it can be tackled, modulated, and mitigated such that the anticipated threat never materialises.

Attempts to realise this promise can be prominently found in CCTV systems that analyse the taped material in real-time, thereby seeking to identify deviant and suspicious behaviour that must be policed and regulated (Macnish 2012); they can be found in known traveller programmes that, in exchange for personal information, establish short-cuts for the immigration procedure at the border, thereby striving to facilitate border crossing for frequent travellers (Muller 2010; Leese 2013); and not least has the dominant paradigm of data collection for the purpose of security analytics been powerfully underscored by the Snowden revelations – exposing to the public how secret services harvest vast amounts of communication and consumption data under the headline of "national security" (Bauman et al. 2014).

The volatility of data as well as constantly augmented networking capabilities radically eradicate the boundaries of nation states and even whole continents. In a globalised world, data travels light and fast, making a person's 'data double' (Haggerty and Ericson, 2000) available for computation long before the actual physical body arrives. Most notably, this principle has become incorporated in Passenger Name Record (PNR) data which contains a large variety of commercial and personal information. Via several bilateral treaties, such data is sent to immigration and security agencies for the purpose of calculating and estimating risk while the passengers themselves are still airborne – or have not even started their travels (Hobbing 2010; Leese 2014; Vermeulen and Bellanova 2012). The process of the European Union's PNR directive that is about to be passed in the near future mirrors the demand for collecting larger amounts of data.

Aviation, more generally, is a prime example for the efforts to create a more secure world through new security technologies as well as through data at scale (Lyon 2003a; 2006; Adey 2003; 2008; Salter 2008a; 2008b). This is not least due to the fact that, technically, many kinds of information about travellers are fairly easy to collect – be it from commercial airlines, from known traveller programmes, or from security and immigration authorities. Efforts to pool such data and exploit it via algorithmic risk analysis have been manifold, and certainly reinforced in the past decade. At the same time, the exchange and recombination of data collected from travellers at various locations in the world brings to the fore the problematic relationship of national legal regimes and global technical possibilities. Given this contextualisation, this case study on "smart security" initiatives in European aviation security is both timely and necessary, and speaks to ongoing research in critical data studies as well as security studies.

Albeit smart security is closely tied to Big Data, it would be misleading to limit the scope of smart security to data processing. Smart security is rather an assemblage of different technologies that are adaptable to the procession of large amounts of data. Proponents of smart security argue that those new technologies, including the use of Big Data, would lead to less intrusive security screenings, more cost efficient security systems, and an increased level of security. Smart security also alters the modalities for issuing appeals against faulty or discriminating security decisions. In a data-driven security environment, the possibility to change individual data becomes a key feature of human rights safeguards and consequently for resistance. If and how these expectations are met by the implementation of smart security routines, and how human rights are to be protected under the condition of data-driven security procedures, will be the subject of this report.

This case study must and will not make representative claims. On the contrary, it might even be argued that representative empirical inquiry (i.e., through quantitative data and statistical analysis) would in fact contradict the idea of a case study that critically examines the idea of Big Data as a neutral, empirical solution for a wide range of (security) problems. It must not be the aim to produce generalisable results, but rather to show which specific challenges smart security poses and how they conflict with existing legislation and policies in the field of aviation security. These examinations will finally result in an assessment of 'how smart is smart security?'

2. Smart Security at the Airport

For a long time aviation in general has been a domain of the rich, the privileged and the military. With the beginning of mass tourism and decreasing costs of flights, air travel became affordable for larger parts of the population. With increasing passenger numbers, potential risks and dangers are assumed to have risen as well. Airports soon had to function in a similar way as border control points do, or with other words, airports put the border in our cities (Virilio 1997). 'Airports must therefore function as a screening or filter for the threats to a nation, but airports also become screens for quite different threats' (Adey 2003, 504).

With the terrorist attacks of the 1970s, planes increasingly became a target that gained high media coverage, as the hijacked El Al flight of 1968 demonstrated. 'Planes were spaces that could be controlled easily; the fear of crashing subduing any passenger resistance. Airports also offered limited surveillance of the throngs of people that were travelling' (Adey 2003, 504–05). The airport and aviation sector responded to these challenges, so that security at the airport became an increasingly important issue. 'Intensified security measures changed the planning of airports, deliberately cutting up the open flow of space' (Zukowsky 1996, 15). Baggage and passenger checks were introduced, but only in 1980, Germany, to give one example, introduced a general law authorising and mandating the federal police to check passengers and their luggage. Until then, this was done based on private terms and conditions of aviation companies and no common level of security screenings existed (Rosch 2014, 60–61).

The attacks of 9/11 were perceived as a challenge to the existing practice of security screenings and several new requirements such as restrictions on liquids in hand luggage were introduced in many countries. Also, there is a trend to introduce better technology and detection capabilities such as security/body scanners or explosives detection, to name just a few.

Another trend in aviation security can be observed: risk based security screenings and smart technologies are not only intended to keep aviation safe and secure, but also to make it more (cost) efficient and preserve the image of fast and convenient travelling at the same time (Adey 2006) – even if the security requirements and passenger numbers keep rising. The statement of Giovanni Bisignani, head of IATA in 2011, is paradigmatic: 'We spend 7.4 billion Dollars a year to keep aviation secure. But our passengers only see hassle. Passengers should be able to get from curb to boarding gate with dignity. That means without stopping, stripping or unpacking, and certainly not groping' (IATA 2011).

In the following section, the trend to a risk based security understanding will be illustrated in more detail.

2.1 From Experts to Big Data: New Modes of Profiling on the Rise

Most security measures introduced in the 1970s were mostly additional checks such as using x-rays or metal detection to prevent dangerous objects from getting on the plane and security officials inquiring or assessing the passengers. During the last couple of years, there are risk based approaches on the rise such as IATA's "Checkpoint of the Future", the CAPPS (Computer Assisted Passenger Pre-screening System) or PreCheck programmes by the TSA (Transportation Security Administration) in the USA. According to a risk based approach, resources at airports that are only limitedly available for security screening processes can be dynamically reorganised in order to focus on those passengers and items that presumably or probably need more intense screening. One reason for that development is that '[a]irport authorities needed a way of putting passengers under surveillance without having to examine every passenger rigorously' (Adey 2003, 505).

Risk analysis is based on today's information allowing a probabilistic prediction of how people will act and behave in the future. As some projects like CAPPS, CAPPS II or PreCheck show, 'such programs generate assessments of an individual passenger's risk for terrorist activity by assigning specific values to particular characteristics, such as method of payment and type of ticket' (Guzik 2009, 12).

This is where not only algorithmic profiling of passengers comes into play, but also the use of huge amounts of data in order to get a picture that is as profound as possible. It is less about the experience of airport security professionals in assessing the situation and behaviour of passengers. 'Where traditional profiling meets its limits owing to constraints in actual knowledge about terrorists and criminals, data-driven analytics go beyond the limits of the known and seek to unveil and rationalize the unknown' (Leese 2014, 501). Algorithmic decisions are on the one hand praised for their lack of racial, sexual or personal bias and are thus assumed to be more "objective" when it comes to the assessment of risk factors (Maguire 2014). The use of data mining and profiling is usually 'justified by arguments of rationalisation' (Rouvroy 2013, 147). Large scale analytics are grounded on the premise that if only we succeed in measuring the world, algorithmic calculations of the ensuing data would enable the world to speak directly to us, thereby circumventing problems of judgement and account that are entwined with human power and authority. The promise of Big Data for the realm of security is a simple, yet tempting one: if we can identify security problems in an unfiltered, empiricist way, we might ultimately get "better" security.

Big Data, thus, can be understood on the one hand as the huge amount of unconnected data items, including even small items such as communication meta-data or location data that may be algorithmically analysed. 'The implicit belief accompanying the growth of "big data" is that, provided one has access to massive amounts of raw data (and the world is actually submersed by astronomical amounts of digital data), one might become able to anticipate most phenomena' (Rouvroy 2013, 143). On the other hand, what makes Big Data so important and intriguing, is that 'Big Data is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets' (boyd and Crawford 2012, 663).

The paradigm of risk assessment or "riskification" in aviation security is not only leading to an increasing importance of algorithms and data analysis, but also to an increasing need to obtain valuable data about passengers. The key assumption in this context is that the more data one has on a person, the better one can assess risk in general. Little or no data is problematic as there is no valuable assessment and analysis possible. It remains, however, rather unclear what "risk" actually means and how it should be assessed. The collection of data becomes an end in itself. Data-mining seems, thus, to be more an axiom rather than a means to achieve a higher level of security.

To get more data and record the behaviour of travellers, 'surveillance has become, therefore, one of the primary means of ensuring that airports are made safe and secure' (Adey 2003, 505). Readability of the traveller is becoming one of the main goals of airport security. '[C]itizenship is (re)designed as "safe" to the extent that the citizen is "becoming digital" and thus "knowable" to the state and non-state authorities allied with the state' (Muller 2010, 77) and where a specific notion of what is to be considered a "safe citizen" is constructed (Muller 2010, 76). Yet it is not only through open or covert surveillance or data collection that information about travellers is obtained, but also through voluntary trusted traveller or frequent flyer programmes like NEXUS or TSA PreCheck in the USA, or airlines' customer loyalty cards. In this context, efficiency does not only play an increasing role when planning and running airport security systems, but also from the passengers' point of view. '[T]he logic of cost-benefit analysis is introduced' (Muller 2010, 79) and travellers are willing to provide more information about themselves in order to reduce 'the long lines and hassle of crossing "thickened", securitized borders' (Muller 2010, 79). Convenience and appearing as a trustworthy passenger is highly valued among travellers. 'And from the perspective of state and corporate authorities, data collection is increasingly regarded as synonymous with greater security, as the logics of governing through risk valorise "governing the ungovernable" and "taming the limit"' (Muller 2010, 84).

2.2 Algorithms – The New 'Decision-Maker'?

The use of data-driven risk assessment is seen as eventually a central part of smart security. Algorithmic security decisions are the foundation for a risk evaluation that leads to real life consequences for the affected passenger. Who is considered to be of high risk is consequently not only up to the discretion of the human operator at a security checkpoint. It is rather the data-driven security decision that builds the foundation for further security screening. This means that algorithms are at the very core of smart security and thus of a new truth regime. Rouvroy calls this altered truth regime, which works through data mining as well as data profiling, 'data behaviourism' (Rouvroy 2013, 146). It builds upon an omnipresent availability of tremendous amounts of data and processes them through algorithms (Rouvroy 2013, 146). Although algorithmic profiling is limited to identifying correlations and computed risk prediction, data-driven security decisions are taken for granted. Data is supposed to reflect the "reality", able to predict "what kind of person somebody really is". This 'data behaviourism' (Rouvroy 2013, 146), however, goes beyond the actual correlation that an algorithm might be able to compute and enters the realm of knowledge.

The code of these algorithms is the law (Lessig 2006) of the truth regime and consequently also of the new way to assess and finally create both security and insecurity. In that sense, security assessments become the result of statistical models which seek to provide high predictability. Collective patterns and not so much the respective individual is of interest in this process. Although each security decision entails consequences for a particular passenger, algorithms need data from as many people as possible in order to create correlations and finally risk predictions. Thus, 'data miners do not want to know who you are but what you are like' (Matzner 2014, 98). Those models exclusively rely on raw data, process them, create statistics and finally build patterns (Rouvroy 2013, 143). Thus, algorithms work on an inductive basis, replacing causality with correlation (Rouvroy 2013, 143). The underlying assumption of this routine is the possibility of getting a sufficient amount of raw data as a kind of digital natural resource to gain robust patterns of risk assessment and eventually future security predictions. It is this reliance on the calculability of the world that seeks to erase uncertainties that have been an essential part of the hitherto notion of security (Leese 2014, 502; Rouvroy 2013, 143).

Data is the resource that is assumed to increase the probability of "right" security decisions. To meet the demand of comprehensive predictive capabilities, more and more information about the greatest possible number of individuals is needed. According to this logic, very different data sources need to be made usable for security routines. Besides voluntarily provided data (e.g. for the TSA PreCheck programme), data gained by state authorities (e.g. census data), by companies (e.g. airlines in the currently negotiated European PNR directive) or from (semi-)publicly available sources (e.g. social media) could also be used to feed algorithms. Data in general have a distinct spatial and/or temporal location and can thus be compared to the very limited and biased perspective of a snapshot or a photograph that deprives the image of its wider context (Amoore 2011, 27). In order to get an idea of the wider picture and to reduce possible biases, smart security algorithms need to rely on as much data as possible. Algorithms use different unconnected data items to draw risk patterns through statistical models. These models identify risk patterns that 'have an aura of "pure" knowledge, autonomous vis-à-vis both powers and effects' (Rouvroy 2013, 148). In other words, data driven risk assessments are supposed to be neutral, independent from any external influence and thus objective reflections of the "reality".

The use of Big Data detaches data items from the individual and redefines them as puzzle pieces in a larger pattern that constitutes notions of normality. The ever-changing data sources that are used to create a security pattern result in a dynamic definition of normality and deviance (Amoore 2011, 29). As risk assessment through probability analyses creates hypotheses on which type of person is prone to be a future threat, the fluidity of the definition of normality results in '*temporary hypotheses* of risk' (Leese 2014, 505, emph. in original). By creating security hypotheses, algorithms ought to make an unknown future calculable. Smart security aims at taking appropriate measures in the present in order to prevent unwanted future events. Given the uncertainty that is connected to probability, algorithms are not suited to precisely predict the future, but they are able to 'render data *actionable*' (Amoore 2011, 27, emph. in original) and finally to bring consequences of future events, that might not even occur, into the present.

In this understanding, algorithms are seen as an objective alternative to subjective human decisions. The decisions of human security personnel can be biased by individual and discriminating prejudices. Algorithms are perceived not to have these subjective biases (Leese 2014, 502–03). They are thus seen as means to overcome racial, sexual, and religious

and any other kind of discrimination. They follow an allegedly neutral code and calculate probabilities. Human limitations in security screenings like subjectivity, attention deficits, the aforementioned biases or individual distraction are a thing of the past. The past subject-based approach is replaced by a pattern-based decision making (Guzik 2009, 7). Risk becomes a matter of probability, is calculable and thus "known". What is not yet calculable due to a lack of raw data, can be made accessible through the exploitation of new sources for data mining (Salter 2008a, 254). By referring to an ever-growing pool of raw data, probability becomes the main paradigm in security assessment. The previous understanding of risk, rooted in uncertainty and the unknown gets colonised by a notion of predictability, or, as Salter stated: 'security chases risk' (Salter 2008a, 254).

2.3 Consequences, Problems, Human Rights Implications

Algorithmic risk assessment based on big data is a highly disputed technology. First of all, it has to be noted that the collected and processed data is not just virtual data, but connected to real life decisions and effects on and power over people. As Lyon (2003, 27) puts it, 'data doubles, created as they are from coded categories, are not innocent or innocuous virtual fictions. As they circulate, they serve to open and close doors of opportunity and access. [...] They make a real difference. They have ethics, politics.'

It is therefore important to look at problematic consequences and features of algorithmic decision making as the effects might be tremendous. In the following, we want to illustrate some of the problems that are discussed in the literature. To start with, we will look at general issues regarding discrimination and structural biases, then focus on faulty decisions and wrong data and finally we will elaborate on the problems of transparency, ways to challenge automatically taken decisions and human rights issues.

General Issues of Discrimination

As mentioned above, algorithmic risk assessment is praised for the lack of prejudices, emotions and unconscious group biases that influence human decision making constantly. However, while computer-assisted decision making is less prone to individual biases, it 'may also normalize the far more massive impacts of system-level biases and blind spots with regard to structural impediments' (Gandy 2010, 33). Unconscious biases and values are written into the codes and algorithms, define which data is collected and how it is analysed. These structural biases are not traceable as the algorithms are not public and might intensify themselves over time and by usage. One might say that all technologies in one way or another discriminate against humans, 'yet, what makes discrimination by an ambient concatenation of algorithmic identifications different is the fine-grained and adaptive spectrum of categorizations that it can produce' (de Vries 2010, 83).

Discrimination by Design

Furthermore, it is not only a problematic side effect of algorithms that they inherit values and biases of the programmers and orderers. Guzik for instance claims that 'predictive data

mining discriminates by design' (Guzik 2009, 12) as its core function is to define and differentiate certain groups that are perceived to be probably more threatening in relation to others. All members of such a statistically singled out group 'bear the burden of this surveillance technique and the innumerable mistakes – false positives – that it will produce' (Guzik 2009, 12). As he points out, this is not just a problem of these individuals being subject to state intrusion which might threaten their civil liberty, but it also affects the fair distribution of these burdens in society as well as privacy and therefore is an issue of fairness or social justice (Guzik 2009, 12). Making decisions based on these categories and groups is called "statistical discrimination". It is often argued that there is no problem in that as long as discrimination along group membership or similar data items provides "better security" by being a reliable predictor even if there is no causal relation (Gandy 2010, 36).

Another point of critique is the kind of self-fulfilling prophecies that investigations and checks based on group membership produce. If members of a group have the same probability of carrying forbidden items as others who do not belong to that group, a higher check rate will still produce more good hits. The resulting statistics will call for even more checks on that group and proof the correctness of the model (Gandy 2010, 38). Thereby, the statistical evidence remains weak, as the overall number of true positive results is extremely low compared to the number of aviation passengers.

Put differently, another inherent discrimination in the usage of these technologies lies in the fact that if one calculates the cost and benefits of its usage, normally only the costs of the responsible institution or decision maker are taken into consideration. But the costs that this usage entails for society are massively discounted.

Human Rights Issues

These costs for society, but in particular for each individual, are the higher the more data-driven profiling is prone to faulty decisions. Hence, the outcome of algorithmic profiling routines is extremely dependent on two factors: the data that is analysed and the analysing models of the algorithm. If only one of these elements is erroneous, algorithmic profiling will produce wrong results and consequently impose real life-consequences on people. Big Data is coined by the use of various data sources. However, the evaluation of the correctness of the data in use goes far beyond the limits of algorithmic profiling. Thus, wrong data will mostly result in wrong security decisions. Another problem lies in the design of the algorithm itself. Incorrect analytical models as well as inadequately chosen variables that are only 'weakly related to the outcomes of interest' (Gandy 2010, 31) will cause a dysfunctionality of the profiling process. That is why both faulty data and dysfunctional algorithms will render algorithmic profiling useless and, moreover, a threat to human rights and passengers' privacy.

Besides these quite obvious sources of failure, there is also a set of problems connected to generating security decisions. One of them is that these data processes are based on inductive reasoning instead of causality. As different algorithms are differently designed and use different and temporarily changing data sources, divergent and even contradicting identifications of risk patterns can occur. Therefore, it is hardly possible to assess which identified future risk pattern to be is perceived as 'correct' (de Vries 2010, 78). Choosing one algorithmic outcome as foundation for security decisions necessarily incorporates a certain level of arbitrariness.

Another problem is that algorithms are programmed in order to identify certain data correlations which result in the creation of risk classifications. This requires a modelling of data that deprives data of its context to fit it into the model of analysis. However, it is often this neglected context that gives a particular data item its special meaning and builds the foundation for further interpretation (boyd and Crawford 2012, 670). While algorithms aim at connecting data to patterns, it is far from certain that every piece of information can be considered as part of a larger picture. Boyd and Crawford state in this context that '[t]oo often, Big Data enables the practice of apophenia: seeing pattern where none actually exist, simply because enormous quantities of data can offer connections that radiate in all directions' (boyd and Crawford 2012, 668).

All these kinds of errors and issues might produce mistakes and lead to faulty security decisions which are often linked to material consequences. A persistent failure in the data on a particular person is, especially in the realm of security, not only annoying, but a grievance that needs to be addressed and corrected (de Vries 2010, 79). However, algorithmic routines are not transparent. They are based, moreover, on rather fluid data sources. The fluidity of data makes both wrong data and erroneous routines hard to identify and hence to challenge (Gandy 2010, 39). Decisions made by algorithms are difficult to assess, especially when security routines do not provide any reasons for their decisions to the airport personnel. In such an environment, the ability for the personnel to question data-driven judgements gets marginalised (de Vries 2010, 82). Inductive methods of algorithms identify a norm and therewith also patterns of deviation by analysing a broad range of data. The 'algorithmic reason' (Rouvroy 2013, 151) thus evades the usual robustness checks like trials or experiments which have been standard evaluation methods not only in science (Rouvroy 2013, 151). 'However, what has been deemed as the overcoming of human irrationality, circumventing interpretation as a source of error and discrimination, then essentially puts data-driven profiling into a black box' (Leese 2014, 503).

Unpacking this black box gets crucial when it comes to human right issues. One of the core civil rights in Western democratic societies is that citizens have the opportunity to challenge state powers instead of being at the mercy of state officials. However, these rights might be at stake when looking at algorithm based decision-making as (1) 'algorithmic governmentality carefully avoids all types of confrontations, especially with those who are affected by its governmental effects' (Rouvroy 2013, 149). People often simply do not know 'if, when, or how they have been discriminated against' (Gandy 2010, 40). (2) If people somehow may discover a discrimination they want to object to, the way this discriminating decision has been made is still in a black box and it is difficult or impossible to trace it back to the algorithm and databases. If one might get access to the source code of the algorithm, it is still very difficult to analyse and differentiate the specific elements of the programme. If we talk about self-learning algorithms, this becomes nearly impossible. (3) Furthermore, the question of accountability remains: Is it the algorithm's, the programmers', or the executing officials' fault? Or does the problem lie with wrong data that constituted the basis for the algorithmic decision making? 'It simply will not be economically or even technically feasible for data subjects to assess and then challenge the "correctness" or accuracy of the data or analytical models used by sentinels, agents, or environments' (Gandy 2010, 39). And (4) if the programmes perform generally well and better than other systems and are validated by authorities, it will be difficult to claim that some citizens are discriminated against by it and that it is not their own fault, e.g. by not providing correct or enough information in order to prevent the system from drawing wrong or discriminating

conclusions. Discriminated people would have to contest a seemingly objective reasoning that has a notion of knowledge and goes beyond mere probabilistic security predictions (Rouvroy 2013, 148).

This means that the same features of Big Data that are praised as objective and independent of human judgment bring about an increasing difficulty to address questions of transparency and accountability of private actors and state powers. Special consideration needs to be given to the fact that algorithm-based decision-making might ultimately undermine binding legal frameworks on non-discrimination and data protection such as the European Charter of Fundamental Rights (Edel, 2010; Guzik, 2009; Leese, 2014; Lyon, 2003b). The possibility to effectively challenge decisions based on algorithmic analysis and the possibility to correct or delete wrong or inappropriate data items lies at the core of human rights and ethical standards are not to be violated.

3. Methodology

In order to understand how data at scale is supposed to become translated into concrete security practices, we used a qualitative approach (Barkin 2008; Gusterson 2008). Qualitative methods are best suited to explore research subjects in-depth, thus enabling researchers to produce a nuanced account of how exactly security is supposed to become 'smart'. Before getting into the details of the study, we will first give an overview of how we set up the research.

We conducted a total number of eight semi-structured expert interviews with eleven representatives from German authorities, airlines, airport operators, data protection authorities as well as NGOs that are active in the field of security and privacy. We talked to the last two in order to include the perspective of affected individuals. Unfortunately, none of the approached representatives of the industry developing smart security technologies was willing to speak to us about their work, some of them with reference to non-disclosure agreements that they signed with industry partners or authorities. This will also be addressed in the following analysis.

When conducting the interviews, we stuck to high ethical standards and best practices which include a complete anonymisation of the interview material, the right not to answer questions and to stop the interview at any time. Interviewees were informed about the project and the form and usage of the information they provided before the interview and all interviewees signed a consent form stating their willingness to participate in the research project.

Interview length was between 45 and 100 minutes. The interviews followed a semi-structured questionnaire and were conducted either in a personal conversation or in a phone call. One interviewee had objections about an audio recording, all other audio files from the interviews were transcribed in order to allow a thorough analysis. The audio files are stored in encrypted folders and will be deleted after the publication of this project report.

In the following sections, we are going to summarise and discuss the findings of the study. The material from the interviews will also be contextualised in a review of existing security as well as data protection policies and their aptitude regarding our results on the socio-technological implications of smart security.

4. Analysis

Rethinking airport security has been on the agenda of airlines as well as airports for a couple of years now. This chapter firstly gives a brief introduction into the genealogy of smart security. Thereby, different elements of the smart security assemblage are presented and scrutinised with regard to their respective ethical and human rights implications. Building on that, the second sub-chapter deals with the three main rationales for the introduction of smart security initiatives: a better security, a better cost efficiency and a better travel experience. Furthermore, questions of lobbyism strategies are addressed. Finally, the third sub-chapter asks for potential modes of profiling and risk assessment smart security routines might use. As it is not yet clear how data-driven profiling might work in the future, different possibilities are presented and scrutinised with regard to their effects on human rights standards.

4.1 The Genealogy of Smart Security

Although increasingly used in security discourses, the term "smart security" remains rather a contested one. This is reflected by the results of the interviews which were conducted in this project. There is hardly any consensus about the specific meaning of "smart security". The interviewees were either not familiar with smart security (Interview 2, l. 85–104; Interview 3, l. 96–101) or considered it a buzzword which is more of an umbrella term than a concrete concept (Interview 8, l. 59–62; Interview 6, l. 53–54). This makes smart security an empty container open for a wide range of interpretations. In contrast to that, three interviewees thought of smart security mainly in terms of the joined security project of IATA (International Air Transport Association) and ACI (Airport Council International). The "Smart Security Project" of ACI and IATA started in December 2013. It continues the work undertaken in IATA's project "Checkpoint of the Future" which started at the beginning of this decade. Also, the ACI conducted a programme to further develop airport security. This programme, called "Better Security", started in 2010 and aimed at making airports more pre-emptive and proactive in the field of security (Interview 1, l. 64-73). IATA and ACI merged their efforts in the "Smart Security Project". However, the "Smart Security Project" 'is still essentially the same project, the same concepts, the same ideas as before under Checkpoint of the Future' (Interview 4, l. 55–56). One interviewee stated that the "Checkpoint of the Future" programme was re-named not only because of the new cooperation between ACI and IATA, but also to get a project name that says: 'You don't have to wait for the future anymore. You can be smart about security right now' (Interview 4, l. 59–60). In contrast to this reasoning, one interviewee from a European state authority was convinced that IATA quit the "Checkpoint of the Future" programme due to quite negative public reactions (Interview 7, l. 12–14). The interviewee was even sure that no-one would currently push forward personalised security screening in Europe (Interview 7, l. 73–74).

Comparing the information material on both programmes, the first reasoning seems to be the more plausible one, as central features included in the "Checkpoint of the Future" project, like behaviour analysis, enhanced detection capabilities, security scanners (probably better known as body scanners) or individual and group-based risk assessment also persist in the "Smart Security Project" (IATA undated, 16; IATA/ACI undated a, 1–2).

The "Smart Security Project" goes beyond the scope of "Checkpoint of the Future" and includes central image processing for baggage as well as new designs for lanes at checkpoints (IATA/ACI undated a, 2). Smart security consequently includes a whole range of means to further develop security routines. It would be misleading to limit the scope of the concept to the concrete programme of IATA and ACI. Rather, smart security has become a more broadly used expression that goes beyond particular concepts. It depicts a new security paradigm. While 'the traditional approach is one size fits all' (Interview 4, l. 121), smart security seeks to deliver more individually tailored security routines. This general definition is probably best suited to illustrate the consequences of the introduction of smart security, as it reveals its very core element. A "one size fits all" approach does not necessitate the collection of any data on individuals, as the same security routine is applied for everybody anyway. A tailored security approach, in contrast, is based on specific information in order to apply a certain security routine to a particular individual. This means, to take the metaphor further, to get as much and as specific information as possible on the objects of security routines. In the case of airport security, these objects are passengers.

Smart security aims thus at collecting or/and using data to meet the goal of individually tailored security routines. Despite most of these security routines needing data to work properly, their introduction has different particular implications. It is therefore necessary, to have a closer look at some of the core routines:

1. *Body Scanners*
   Body scanners detect hidden objects underneath the passenger's clothing. They have been subject to extensive critical research (Leese and Koenigseder 2015; Valkenburg and van der Ploeg 2015; Bellanova and González Fuster 2013). Today, there are more than 1,000 body scanners installed at checkpoints in various airports around the world (IATA/ACI undated b, 1). Body scanners detect metallic as well as non-metallic items carried underneath the clothes. One interviewee mentioned that body scanners could be equipped with a variety of screening algorithms that deploy different screening intensities either on a random or on a pre-determined basis (Interview 4, l. 510–13).
   Proponents of the introduction of these new security devices claim that they 'reduce the need for intrusive pat-downs by automatically locating concealed objects and minimize privacy concerns by displaying an anonymized stick figure rather than detailed images of the body' (IATA/ACI undated b, 2). Though this description sounds quite tempting in terms of privacy as well as of security, it neglects the problems that are linked to the introduction of body scanners. One ethical problem is that body scanners identify prostheses, hidden disabilities as well as medical devices and expose people who are in need of them to a higher probability of being subject to more severe security checks. Also transgender people are very likely to be discriminated against by body scanners. Body scanners thus, as a second problem, amplify societal notions of normality and deviance and foster the stigmatisation of people who do not correspond to pre-determined categories of being normal.

2. *Centralised Image Processing (CIP)*
   CIP is another yet less problematic means in the context of smart security. It works through a physical network between the x-ray devices at the checkpoints and one separated central space where the x-ray images of more than one lane can be processed. This technical innovation could lead to a more efficient baggage

processing, as the security personnel will be able to analyse images without the usual distractions at the checkpoint. It moreover minimises unused capacities. As CIP increases the number of processed x-ray images per hour, it contributes to a higher cost efficiency. It turned out in the interviews that this, and not so much a potentially increased level of security is the driving force behind the introduction of CIP (Interview 4, l. 211–30). This technology has been introduced for example at Amsterdam Schiphol Airport (IATA/ACI undated c, 1).

3. *Behaviour Analysis*
   Smart Security also embraces behaviour analysis of passengers as a security routine. This means that 'both positive and negative passenger behaviours can assist in the evaluation of an individual's risk and their potential intent to commit unlawful interference on board the aircraft' (IATA/ACI undated a, 2). While positive behaviour could lead to a faster processing, negative behaviour would cause more intense security checks. Behaviour analysis is currently thought to be 'undertaken by trained individuals' (IATA/ACI undated a, 2). Given the sheer mass of people at checkpoints, a potential selection bias of the personnel needs to be examined further. This bias could lead to discrimination, especially when prejudices come into play.
   However, behaviour analysis could also be supported by camera systems (Interview 5, l. 1069–72) which raises a range of additional questions in terms of privacy and normalisation. Behaviour analysis could lead to an increased assimilation of passengers' behaviour. That means that passengers behave in a way to meet unknown and unspecific criteria thereby restricting themselves to a probably unnecessary degree. Although behaviour analysis might not be a very visible security means, it is still a rather intrusive one that needs to be subject to further ethical scrutiny. It was furthermore also contested among our interviewees if this method works reliably at all, bearing in mind a large set of reasons for deviant behaviour like fear of flying (Interview 5, l. 1088–91).
   While behaviour analysis is a taboo in Europe (Interview 5, l. 1082–83), it is currently deployed in the United States (Interview 4, l. 312–14).

4. *Risk-Based Security*
   The checkpoint at the airport is supposed to become dynamic such as to be adaptable to different risk-categories. This differentiation is supposed to lead to an increased throughput of passengers in order to make checkpoints both more cost efficient and more effective in terms of security screenings. This can be achieved through different approaches. One is to identify rules (e.g. ticket purchasing modalities). Others could be the adaptation of the screening level according to the risk classification of a certain route or a certain category (like age). Risk-based differentiation could be finally conducted through the consideration of pre-screening results (e.g. explosive trace detection) or the above mentioned behaviour analysis (IATA/ACI undated a, 2). According to our interview partners, a random component should additionally always come into play to reduce the predictability of the security checks (Interview 4, l. 535–37; Interview 5, l. 513–15). Depending on the concrete approach of risk-based security, there are different ethical implications. While category-based sorting might entail a discrimination due to the design of the single categories, others, like purely random approaches, are less problematic.

These four elements of smart security are just examples of a whole assemblage of security innovations, also including lane design, cabin baggage screening solution and checkpoint real-time monitoring that, taken together, form smart security (IATA/ACI undated a, 2). The introduction of most of them raises ethical and human rights questions, like briefly outlined in the examples above. This is already the case when these means are regarded as separate technologies. The example of behaviour analysis as one approach of risk-based security illustrates, however, the interconnectedness of the different routines. This becomes even more problematic when the use of data comes into play through a data-driven approach. Although this is most intuitive for risk-based screening, the use of a variety of data sources in the security checkpoint environment at airports is possible for virtually every checkpoint component. Integrating Big Data into the security checkpoint has rather remarkable consequences. While security items like x-ray devices, body scanners or behaviour analysis generate data in order to allocate passengers to risk-levels, data-driven algorithms use these and other data in order to conduct such an assessment. The interaction of the before-mentioned routines can create reliable security routines. One interviewee compared the different layers of security at the airport with several slices of Swiss cheese:

> *'[T]he point is, if you have three slices, one after another, and each one has holes in, you could probably find a position through which you could actually go through. So the point is that if you knew the system, if it was a static system, you could still find a way around it or a way through it. If the slices would be moving all the time, you could not find a way through it.' (Interview 4, l. 531–35).*

This dynamic system of security relies on a high degree of unpredictability and is not necessarily tied to the use of large amounts of data (Interview 4, l. 524–25). However, the implementation of data-driven routines remains an envisaged goal of some actors in the field (Interview 4, l. 110–16; Interview 5, l. 250–73). This development brings a lot of questions to the fore that need to be examined. In a first step, the next chapter analyses the motivations and the main actors in the development of smart security. In the following, we will not take all the different parts of the smart security assemblage into account but focus on the data-driven risk assessment and passenger differentiation.

4.2 Driving Forces and Goals of Smart Security Initiatives

The concepts of smart security initiatives are mainly based on three goals that are expected to be reached or approached by introducing new security measures and changing the system of security checks. '[T]he idea of smart security is really to find the vision to find a new way from curb to airside' (Interview 5, l. 462–63). Security checks and the process of getting through the airport and on the plane should become '[…] more secure, but at the same time more efficient, meaning faster, and possibly cost-efficient. But also a better experience for the passengers' (Interview 4, l. 27–29). It is these three objectives that are named when talking about the reasons and visions behind smart security initiatives: Better security, increased cost efficiency and a convenient travellers' experience. In the following, we want

to look deeper into these logics and set them into context by comparing different takes on smart security.

4.2.1 Better Security

When referring to the introduction of a different and better security level for aviation, proponents of smart security compare the ideas of new technologies and risk based passenger differentiation with the current security system that is seen as a model from the 1970s and 80s and has not been changed profoundly since then (Interview 5, l. 464–65). By introducing smart security systems, not only does one introduce better technology for detecting dangerous items, but also risk based differentiation of passengers and discrimination into high risk and lower risk passengers. It is argued that by differentiating into these categories, one can focus on high risk passengers in order to make sure that especially they are not carrying anything dangerous.

Actually, when looking at the reasoning it quickly becomes clear that better security is only one and probably not the most important reason for pushing for smart security. Very quickly, interviewees proposing smart security came to other topics after talking very generally about security, such as: 'We have a keen interest in security, we don't like our planes falling out of the sky.' (Interview 4, l. 15–17); followed by: 'And we have a keen interest in our passengers having a good experience when they travel' (Interview 4, l. 15–17). Another interviewee observed that the moving force behind smart security initiatives 'is mainly economic reasons and the search for more comfort, not security considerations' (Interview 7, l. 70–71).

Most interestingly, several interviewees stated that in Germany, the police has a different take on smart security than airports and airlines as the authorities are quite content with the security system as it is in general. 'The police do not demand nor introduce a risk assessment of passengers' (Interview 7, l. 44–48) and 'passenger differentiation is not planned to be introduced in Germany' (Interview 6, l. 383–85). In fact, it is even doubted that data driven approaches in aviation security in order to do risk assessment are a useful and rational way of improving security as '[t]here are much better measures than collecting data which could be deployed earlier if one wanted to raise the security level even higher' (Interview 7, l. 122–24).

While not sharing the same opinion on the need for passenger differentiation, police and law enforcement, airports and airlines generally want to 'optimise existent procedures to make the checks easier' (Interview 6, l. 466–67) and to introduce and work together on better and smarter technology, e.g. for baggage screening by x-ray machines or people-screening by the security scanners introduced recently.

To sum up the security argumentation one can observe that although better security as a reason is often named first when pushing for smart security, it is not clear and also disputed where exactly the increase in security can be found within smart security. Interestingly, the police in Germany apparently opposes data driven risk assessment, however, better technology and smoother security screening installations are welcomed by many stakeholders in aviation security.

4.2.2 Better Cost Efficiency

The second reason that is driving the proposals and implementations of smart security measures can be found in the aim to seek better cost efficiency for airports and other aviation stakeholders. It is said that 25% of some airport's budget is spent on security and that the current '[…] system will not be sustainable for the next 20 years' (Interview 5, l. 431–32). Airports even expect increasing security costs as passenger numbers keep rising. In fact, it is expected that the number of passengers will double until 2035 but it is impossible to double the airports in order to keep the same security system working for these numbers (Interview 1, l. 75–77). Therefore, smart security wants to reform security procedures in order to lower the burden of security costs. 'The point is that there is no way you could screen every single passenger for every single threat all the time. Because it will be too costly, it will take too much time, it's just not going to work. It's going to be a burden. So, I think that's the "smart" in smart security' (Interview 4, 125–31). The aim is 'to develop a long-term vision with a long-term solution. Also for airports to plan their infrastructure and their costs. So that's the thing' (Interview 5, l. 726–28). One interviewee found very clear words on the relation of security goals and saving money when stating that '[…] the idea of the risk-based differentiation at the end is to keep the security level as it is, but for airports to gain some operational efficiency; and at the end some cost-saving' (Interview 5, l. 574–75).

Interestingly, other interviewees doubt the cost saving effect of data driven smart security as the data collection, storage and analysis involves high setup and maintenance costs. One interviewee claims that 'no calculation on costs of data collection and analysis has been done' (Interview 6, l. 296–306). The cost and calculation depends of course on the question of who is in charge of collecting and assessing the data. If this task is not allocated to the airports or airlines but to the governments, airports and airlines may save expenditures due to reduced costs by differentiating passengers into categories while governments have to take care of the data management.

To summarise, the argumentation on better cost efficiency is much more elaborated and seems to be a more important driving force behind smart security initiatives than the aim to enhance security at airports.

4.2.3 A Better Passenger Experience

The third goal of smart security is 'to provide a more comfortable travelling experience at airports and to reduce the burdens by controls' (Interview 7, l. 10–11). The idea is not only to install quicker screening technologies and optimise the processes of security checks, but also by differentiating passengers and sorting them into different risk levels to 'reduce the number of [security] lanes' and to 'expedite the security [screenings]' (Interview 5, l. 77–79). The ultimate goal according to one interviewee is that normal passengers and passengers participating in known traveller programmes arrive at the airport, identify themselves automatically via their biometric passport and only 20% of them, randomly chosen, will have to go through the ordinary security checks. The vast majority of 80% is asked to only do a 10 seconds explosive items check. 'You don't go through x-ray with your baggage, you do not open the things' (Interview 5, l. 186–90). Those passengers would experience 'a lighter screening' (Interview 1, l. 107). The basis for this is a 'risk assessment before you come to the

airport' and not a "one-size-fits-all" security setup (Interview 5, l. 306–08). This would lead to much less hassle and time consuming security checks for most of the passengers thereby also saving money as people can go through security more quickly (Interview 1, l. 113–15). 'And also, you're being less intrusive and less invasive to those people who have decided to apply for pre-check' (Interview 1, l. 115–16). The aim is therefore, with the help of smarter technology and passenger differentiation, to make the security checks more acceptable for passengers and also to make them quicker and less costly.

4.2.4 Whose Initiative?

After illustrating the main goals that are mentioned and put forward when talking about smart security, we want to look more into the interests and actors that put forth this reasoning.

What we could see relatively clearly is that smart security is at the core of the future of airports. For airports, the most important goal is, according to our interviews, to keep the costs of security low. It also has to be taken into consideration that airports are sometimes seen as 'the key players in aviation' (Interview 5, l. 28). 20 years ago, it used to be the airlines telling the airports what they want. 'Today, […] it's the contrary. […] [A]irports can decide what they want' (Interview 5, l. 29–30). Airports are also seen to be in a good position to lobby for their ideas and interests, as 'there's a lack of vision of the [European] Commission for the time being' (Interview 5, l. 804) and therefore 'a good timeframe' (Interview 5, l. 804–05) for the industry to tell the regulators what they want as '[t]he Commission doesn't exactly know where they want to go' (Interview 5, l. 804–11). But airlines generally do not have the same interests that airports have (Interview 5, l. 841–43). As far as we can see, airline representatives are more interested in providing better travelling experience by reducing time-consuming and intrusive security checks as well as keeping their planes "up in the sky".

Data driven approaches are not as important for airline representatives as for the airport representatives we talked to, but they are very much interested in new technologies that ease the passenger flow. For airlines, security checks are just one component of the travel experience that could make it either more or less convenient. Airports, however, have to spend money on new security means, need to provide the new devices with sufficient space and to allocate the personnel for running the checkpoint. This is why airports and airlines have some different interests, although they are often, in fact, working on the same page when it comes to security. This is probably best illustrated in the cooperation within the "Smart Security Project".

We also tried to talk to industry representatives working on the specific implementations regarding both the technology part of smart security and the algorithm-based data-driven part. However, we were denied access to interview partners from the industrial sector. Some were reluctant to talk about their work as they had signed confidentiality agreements with industry partners. We know from the other interviews that the aviation security industry is cooperating with airports and airlines in pilot projects of smart security, e.g. at Amsterdam Schiphol (Interview 1, l. 128–29) or London Gatwick, and also with law enforcement agencies on developing technologies. We can only assume that the industry is eager in promoting

smart security solutions (Interview 8, l. 141–50) but we have no definite information on their lobbying activities.

What we can conclude from the interviews we conducted, though, is that airports and airlines are publicly promoting an individually tailored smart security screenings and also lobby on the European level. The police representatives we talked to, on the contrary, argued that they welcome and work on better screening technologies, but they do not want to push forward a data-driven security approach. They rather promoted an equal treatment of all passengers (Interview 6, l. 353–54).

4.2.5 Achieving a Mind Shift towards Smart Security

Lobbying is probably one of the most relevant tools in order to introduce smart security routines at airports. That is why airports and airlines as well as their associations are trying to influence state bodies and organisations in the field of civil society. For airports and airlines questions of cost efficiency are the driving force behind their lobby efforts. Introducing known traveller programmes could thereby reduce the intensity of security checks that are necessary for registered persons and thus reduce the security expenditures of airports (Interview 5, l. 73–80). Another interviewee added that airlines also have a keen interest in reducing bottlenecks at the checkpoints, in order to increase the throughput per lane, therewith reducing costs and simultaneously creating a better travel experience (Interview 4, l. 240–68). It is thus industry associations that 'try to advocate certain approaches with regulators' (Interview 4, l. 609–11), for example on the European level (Interview 4, l. 616–18).

But not only industry associations lobby on the European level. NGOs also try to influence the European decision-making process. According to NGO representatives, especially the European Parliament is rather open for the NGOs' point of view (Interview 3, l. 446-56). In contrast to that, it is more difficult to bring NGOs' perspectives, which are predominantly concerned with human rights issues, into the negotiations of the Council of the European Union that consists of representatives of the 28 EU member states. One interviewee explained that by assuming that the member states focus more on their national interests including national security (Interview 3, l. 459–62). As security is primarily still a national policy field which is difficult to approach for NGOs, this is a strategic disadvantage for NGOs and thus for human rights lobbyism.

While behaviour analysis is still a taboo among EU member states (Interview 5, l. 1082), other means enlisted in the "Smart Security Project" gain increasing support. The best example of this is probably the 'SURE!' project at Schiphol airport in the Netherlands. '[W]hat is unique about them is that you have a regulator, an airport, and then KLM as the main airline there, that are completely on the same page and are working very closely together' (Interview 4, l. 671–73). But not only the Netherlands, also are the United Kingdom and France open to the field of smart security. In the United Kingdom, Heathrow airport in London is testing smart security devices, although they 'are a little more conservative in their publicity and what they say to the outside world' (Interview 4, l. 736–37). Also in France, there is a smart security programme called "Vision Surté" (Interview 5, l. 868). These few national programmes are considered by industry associations to be not only testing

fields for the future airport security but also advertisements for smart security routines among other countries (Interview 5, l. 864–68). Other countries like Germany, however, are more reluctant 'when it comes to elements of risk assessment and data privacy' (Interview 4, l. 695–96). Another interviewee confirmed that impression by stating that Germany predominantly uses technology and not personal data in order to process security checks (Interview 6, l. 198–205).

On the whole, the acceptance for smart security is 'moving very slowly in Europe' (Interview 4, l. 483). Only 'some European countries have stated some interest' (Interview 4, l. 863). However, the implemented programmes in the United Kingdom, in France and especially in the Netherlands show partially increasing interest in smart security. While cost reduction is the driving force of the aviation industry's lobbying for smart security, other rationales, like the enhancement of the security level, are brought to the fore as well. Although promoting smart security, some of the interviewed actors found it quite difficult to generally assess if smart security entails security improvements (Interview 4, l. 172–83).

Additional to the lobby activity for smart security, one interviewee mentioned another strategy to generate a mind shift that ultimately might foster the widespread introduction of smart security devices. This strategy aims at introducing known traveller programmes where passengers give their data voluntarily in order to have quicker and less intrusive security checks (Interview 1, l. 115–16). Several interviewees mentioned that this could become the first step in implementing data-driven security routines. This, so the rationale goes, would increase the openness for data-driven security checks (Interview 1, l. 110–18; Interview 4, l. 477–79; Interview 5, l. 367–69). The general introduction of data-driven profiling would be a potential future expansion of then existing mechanisms (Interview 5, l. 368–69). In other words, known traveller programmes would serve to circumvent today's reluctance in implementing data-driven profiling.

In the past few years, most of the work has been done in the field of security technology. This work has predominantly aimed at 'optimising security processes and the equipment at checkpoints' (Interview 1, l. 101–02) and now slowly makes some governments think about how to use data in order to differentiate people in the context of security checks (Interview 1, l. 102–04). An interviewee added that, in the meantime, industry has started to develop algorithms, e.g. for the support of x-ray analyses at airports (Interview 5, l. 1027–36). Given these ongoing developments, the introduction of known traveller programmes such as the EU's proposed Registered Traveller Programme would serve as a perfect base for a future mind shift towards data-driven profiling through the backdoor.

4.3 How Smart Security Works

After evaluating what is understood by smart security, where it comes from, which aims it embraces and how it is planned to be brought into functioning, we now want to shed more light on the data-driven parts of smart security. We want to know how exactly the algorithmic decision making is supposed to work, what features it encompasses and also, which problems and obstacles are seen and how they are evaluated. Therefore, in the first part of this chapter we look at the data sources that are to be used. In the second part we illustrate the methods of risk assessment that might be deployed, and the third part deals

with accountability problems linked to data-driven profiling. Finally, we analyse the problem awareness of relevant actors in the fourth and last part of this chapter. Examining what problems are identified by the stakeholders involved and how they deal with the consequences of the revealed obstacles is a key element for understanding the human rights implications that the introduction of data-driven profiling entails.

4.3.1 Profiling as Part of Smart Security

The ideas about which data should be used to form a basis for risk assessment algorithms are not coherent and we observed several also very conflicting opinions. The interviewees who are in favour of more risk based security share to a certain degree the idea that existing data such as Advanced Passenger Information (that some states request from travellers before entering the country) including passport details or data that airlines already have should be used. As one interviewee put it, the idea is to 'pool existing data […]. Potentially, that same data can be used to give information to the passenger. It can be used at the same time to give information to border force and to the security elements of the airport. So, the bigger project is how can this data be used, and how can we re-use the same data for multiple entities' (Interview 4, l. 111–14).

Another data source is the data that is collected and stored in Passenger Name Records (PNR). PNR data includes about 60 items such as information on the route, from the booking process (such as credit card data), meals and seating details from the flight and a lot more. This data is already collected according to some agreements between several states. The European Union is currently in the process of passing a PNR directive in order to require the data of all flights entering the EU or, eventually, inside the EU to be collected, stored and shared with EU member states and, potentially, eligible partner states. Proponents of smart security also see PNR as very useful for profiling and risk assessment as 'then there might be an opportunity to actually try to identify passengers of greater risk or actually passengers of lower risk' (Interview 1, l. 119–20). 'If governments are going to collect these data anyway from a border control perspective, […] why then not make the best use of them and use them also to the benefit of the passengers, for security purposes' (Interview 4, l. 439–42). However, some interviewees stated that the use of PNR data is probably restricted and it is not clear if the proposed or already even passed text of the directive would allow for the use within a smart security framework.

What all supporters of smart security proposed is the introduction of a known traveller programme similar to TSA PreCheck in the USA where travellers voluntarily provide information about themselves. Some mention additional background checks on these travellers that could include very different measures. One interviewee could imagine that a check on political memberships and activities could become part of a background check done by intelligence agencies (Interview 1, l. 258–64), another did not use those specific words, but stated similarly that 'if somebody has a good job, has a good income and has a family, and everything's fine, well, then they're very unlikely to do something stupid' (Interview 4, l. 424–30). In order to do that, one interviewee suggested to use a 'kind of travel history, or work history as well, [of] the last five years' (Interview 5, l. 253–55). The problem would then be, according to another interviewee, that 'governments probably couldn't afford to go there, from a political perspective, [b]ut there are approaches […] where with a

fairly limited amount of data you can at least get some indication on more or less probability and certain people that you might want to have a second look at' (Interview 4, l. 424–30). According to this statement, it would be desirable to single out people based on their way of life/their social reputation, and to sort them in order to optimise the security throughput. The conclusions that can be drawn from that kind of statistical information being checked against predetermined notions of normality, are far from being "objective knowledge". They rather represent very subjective ideas of what a normal and harmless way of life should look like and thereby, which behaviour is deviant and at the same time suspicious.

Nearly all proponents were additionally open to use (semi-)publicly available information such as the information of a Facebook profile since from there one 'can learn a lot about the person' (Interview 5, l. 272–73). Also behaviour analysis, enriched by CCTV footage of airport surveillance, can be part of the data sources that are used for assessing passengers risk levels. Furthermore, information gathered could and should 'be cross-checked against check lists and intelligence watch lists' (Interview 1, l. 108–09).

Given that vast range of very diverse imaginable data sources that form the baselines for risk assessments, it is quite stunning that there was not very much awareness or discussion about data that should or could not be used from an ethical or human rights perspective. While some interviewees said that this should be assessed by the governments, others just answered that they 'don't really know actually' (Interview 1, l. 168) or answered that ethnicity, for instance, normally is not part of the database: '[P]rofiling doesn't use race, religion, or nationality. It looks at what you've done and what way you've been and how you've done it' (Interview 1, l. 179–81). The question remains: If so many different data sources are combined, how could it be assured that nationality or proxy data that hints at race or religion (Interview 8, l. 535–49) is excluded from being part of the analysis?

Quite stunningly and also very much opposed to the idea of a cost saving, large-scale automatic data analysis framework that we are talking about, we also came across the firm view from a proponent of smart security who wanted to combine the data-based background check with a proper personal interview (Interview 5, l. 255) and 'a security awareness questionnaire online' (Interview 5, l. 203–04). According to this view, it is not only the data about a person that is important, but: 'we need to see you' (Interview 5, l. 262–63).

Not only the data sources and different ways of data collection have to be thought through when planning a smart security system. Also the question of who is analysing and storing this data is of great interest. Most proponents of smart security assured that the databases are to be run by the governments who are also in charge of doing the analysis (we will come back to the way of analysing later) as 'that's really what governments do, that's not what private industry does' (Interview 1, l. 270–74). However, it is not completely clear how the roles of airports and government agencies in storing and analysing data are planned to be organised. The statement of one of the interviewees demanding that airports should 'not be the last one to use it, because everybody is already using it. The airlines are using it, the border is using it, everybody is using it' (Interview 5, l. 99–100) is suggesting that also airports should have access to the data. The final aim of this interviewee, however, is to 'have just one database with all the data about you and then it's easier' (Interview 5, l. 1007–08).

Taken the information we could gather about data use and storage together, we can see that there is no coherent concept observable right now. The ideas of collection reach from

privately gathered information e.g. by airlines, to a combination with databases required by the government like PNR as well as behaviour analysis and thorough intelligence-led background checks. We cannot see an adequate reasoning on the kind of data sources and items that are to be included or should not be included as for example put forward by data protection authorities. Furthermore, there is no awareness observable that according to European data protection law, data about citizens cannot be easily reused for a different purpose without the consent of the affected citizens.

4.3.2 Risk Assessment

After having investigated the proposed and foreseen ways of data collection and storage, in the following we will take a look at the concepts behind risk assessment, the working of risk assessing procedures and the consequences and aims thereof.

At the core of the risk differentiation lies the question of who is going to define what "risk" is and how that definition will look like. With regard to the question who is in charge of risk definitions, most interviewees were convinced that this 'will be up to the regulators, to governments to decide how they do this. I think as industry, this is way too sensitive for us to get involved in' (Interview 4, l. 359–60). Airports can have their 'own local risk assessment. But then it's the states, the intelligence agents, the police, or the CIA, I don't know' (Interview 5, l. 947–48).

When talking about the aims of risk assessment and about the expectations connected to passenger differentiation, in fact, very different and inconsistent opinions were put forth by proponents of smart security. First of all there are the two conflicting ideas whether one should focus on the low risk and identify passengers with that characteristics (e.g. Interview 5, l. 687–88) or to 'pick out the bad people who're on the bad objects, and trying to see if we could identify those passengers who were a higher risk […] or potentially higher risk, should we say' (Interview 1, l. 80–83). One reason for these contrary approaches could lie in the fact that 'no one is actually doing this in a live environment, but they are starting to look at it. […] And it seems that some regulators seem to be a bit more comfortable using the data to increase security, not to decrease it' (Interview 4, l. 401–05). However, 'because it's just a slightly different approach' (Interview 4, l. 401–05) it would be no problem to then single out the low risk passengers and decrease the security checks for them so the envisaged cost efficiency finally comes into play.

Secondly, there is no coherent idea regarding both the aim of identification (low risk or high risk) and how many different categories should be set up and passengers sorted into. The "Checkpoint of the Future" proposed three categories: high risk, normal risk, and low risk/trusted travellers. But as we did the interviews, an airport representative opposed that model of risk levels and proposed a two-levelled model that would only sort into low risk/known travellers with less checks and the others that have to go through normal checks. We also came across another category that is not officially communicated but popped up several times in the interviews: people who are not allowed to board based on their risk assessment. This will lead us to the discussion of the consequences of risk-based passenger differentiation.

Again, there is no coherent image of the consequences passengers have to expect based on the result of the sorting algorithm. Interviewees kept reminding us that even if they were looking for higher risk persons and giving them a special treatment, 'the impact of it isn't going to be that high. […] [A] different algorithm would be run, and you wouldn't even know that it was a different algorithm' (Interview 4, l. 894–99). This is done for instance by putting a marker on the boarding pass so that only the security personnel would recognise that the passenger is to be treated differently. '[E]ven if you are selected, the impact is maybe [that] you're delayed by two or three minutes' (Interview 4, l. 905–06) as 'you have [a] slightly [higher] chance that the alarm went off because it was more sensitive, and therefore you would have to go through another step of security screening' (Interview 4, l. 894–99). Thus, if you 'have been identified as a passenger that needs to be screened to a high level, you really don't have much visibility of that. Which means, you're not going to feel that you have been profiled, or unfairly' treated (Interview 4, l. 575–78).

The consequences for passengers allocated to a low risk category would be to get quicker screening compared to normal travellers, while travellers of higher risk would have to go through additional or more sensitive checks. Interestingly, although interviewees were highlighting that the impact and consequences of the risk assessment are not necessarily noticeable and also not something to worry about, there is obviously also the potential consequence not only to have the higher chance for more thorough checks (which lead also to a higher chance for finding forbidden items as shown above in the theory section and therefore reinforcing the legitimacy of special treatments), but also to be declined to board the plane. An airport representative stated that there is a democratic right to fly even if assessed as a high risk person and if that person is not carrying dangerous items (Interview 1, l. 201). On the contrary, an interviewee affiliated to airlines argued that '[f]rom an aviation security perspective, […] if we think he poses a threat to the flight, he should not get on the flight' (Interview 4, l. 389–90). In different words, the same interviewee stated that 'people that have elevated risk […] we're not going to allow to fly at all or we're going to really scrutinize them before they go on the plane' (Interview 4, l. 307–09). It becomes clear that the consequences of being sorted into an category of higher risk does not necessarily lead only to a security check that takes two minutes longer than the standard one, but it can lead to real problems including being denied to travel. This becomes even more problematic if this information is stored in data bases and used again for different purposes. What if a person who was denied to board a plane wants to rise his/her credit limit? What if he/she applies for a job?

Given the possible consequences of a risk based passenger differentiation, it is important to know and to evaluate how this risk assessment is accomplished, which factors play a role and what kind of idea or algorithmic programming is implemented. As this is the core of the whole process of smart security, we were quite surprised of how little knowledge and insights people that propose smart security could give on that topic. While, on the one hand, one interviewee stated that they did a 'lot of thinking around' the question of who is in charge of a risk definition (Interview 4, l. 358–59), the questions around data sources, working of algorithms and risk assessment strategies, on the other hand, is 'an area where we haven't, to be honest, progressed a whole lot, because of its sensitivity' (Interview 4, l. 284–85).

However, we could get some basic ideas at least. Before risk assessment systems are going to be installed, interviewees suggested that one could start with risk assessment based on

travel routes (Interview 5, l. 180–82). This can also be done without the collection of passenger data and is a form of deductive or pattern based risk assessment. In fact, when we wanted to know more about the concrete working mode of the algorithms, we just heard that there is 'definitely' (Interview 5, l. 1126) no discussion at all about different forms of algorithmic analysis. It, thus, remains quite unclear whether passengers that fit into predetermined patterns are to be singled out or whether one wanted to "let the data speak for itself" via self-learning algorithms that inductively derive a range of more risk-prone passengers. Furthermore, we were referred to the regulators as they should know, but not the people that are lobbying and pushing forward on its introduction.

The examples given by the interviewees describe a riskless and "good" traveller by means of being "normal". One example given was about clothing and that normally, if you wear casual clothes when travelling you should have some luggage with you, otherwise this would be suspicious (Interview 1, l. 218–20). Buying your ticket in cash last minute, or having a travel history including destinations of the Middle East (Interview 1, l. 142–45), on the opposite, is seen to be not normal, but perceived as markers that would add to the level of risk and suspiciousness. Again, this mixes ideas of a normal travel history with pre-defined patterns such as defining specific travel destinations as contributing to a higher risk level. These all would function as markers and 'it wouldn't necessarily say they're guilty of anything' (Interview 1, l. 196–98) but it would be taken into account to calculate the risk level. However, nobody knows which data is relevant for a thorough risk analysis: 'That's the million dollar question, right?' (Interview 4, l. 353).

5. Ethical Implications of Smart Security

Even if data-driven profiling is in an early stage, several ethical implication arise out of the use of large amounts of data in algorithmic security routines. This chapter starts by analysing accountability problems in a checkpoint environment that includes human operators as well as data-driven security practices. The development of smart security means needs to be based on a high level of problem awareness. The second part of this chapter, thus, scrutinises how proponents of smart security are aware of ethical and human rights aspects that are affected by smart security. It thereby becomes obvious that smart security needs to be subject to a public debate on what airport security should look like and which level of security is desirable at all.

5.1 Accountability and the Possibility of Resistance

The use of data-driven profiling is always linked to the question of accountability. Depending on the specific design of data driven-profiling, different problems come to the fore. Inductive methods create a statistical norm and consequently also categories of deviance. They define what is normal, and thus unsuspicious, by analysing data and creating patterns with the aura of objectivity (Rouvroy 2013, 148). As inductive routines process a large amount of data in order to generate their patterns, the outcome always depends on the data that are used. Biases in data selection influence the outcome and finally the intensity of security checks for a particular passenger. However, due to the fluidity and the dynamics of data sources, it is hardly retraceable on what basis temporary notions of normality have been defined. Many algorithms are not transparent. This causes severe problems in terms of accountability. It remains, for example, rather unclear whether an inductively working algorithm created a discriminatory security decision which causes more intrusive security checks for passengers that do not fit into the definition of being normal. The individuals affected would not have any evidence of being discriminated against, as they do not know how the security algorithm works and the use of which data sources led to the potentially discriminatory security decision and practice. As inductively created forms of normality are both hard to retrace and hard to question, a severe accountability problem arises.

Deductively working algorithms, on the contrary, use categories to determine the risk level of a particular passenger. It might be possible to prevent the deployment of explicitly discriminating rules and categories. However, the definition of rules is shaped by a certain perspective on the world and thus includes personal biases. The mere building of categories is thus always linked to either positive or negative discrimination. Security categories thus reflect a subjective understanding of the rule-maker. Even if these categories are built upon experts' experiences and/or statistics, they still have an arbitrary element and remain security hypotheses which assign a particular person to a pre-defined security category on the basis of certain assumptions.

In contrast to inductively working routines, deductive algorithms can be checked on the basis of their underlying rules. This gives affected individuals at least a chance to raise objections against security decisions. This is, yet, by far neither a guarantee for a non-discriminatory working security routine nor for a non-discriminatory outcome (Gandy 2010). Despite deductive rule-based algorithms having slightly less accountability problems compared to inductively working ones, the use of data-driven profiling is always to a certain degree fuzzy when it comes to the question of who actually holds responsible for a particular security decision.

Our interviewees disagreed whether security personnel at airports should be informed about the exact functioning of data-driven profiling. The preferences, even among people working in the same sector, range from extensively trained security personnel to completely uninformed human operators (Interview 1, l. 472–75; Interview 5, l. 493–94). No interviewee neglected the necessity of human security personnel at checkpoints. However, the operators' capacity to assess security decisions decreases with decreasing knowledge about the functioning of algorithmic profiling. As algorithmic decisions are often taken for granted and assumed to be correct, human operators will mostly accept them in an unquestioning fashion. Consequently, the ability to question data-driven security decisions is dependent on how much the security personnel actually know about the functioning of the smart security devices and algorithms. Despite interviewees from both state authorities and aviation associations partly expressing their preference for uninformed operators in order to reduce human biases in the decision-making process (Interview 1, l. 472–75; Interview 7, l. 107–12), their level of knowledge directly affects their ability to critically assess algorithmically made decisions.

But even if the security personnel understand how algorithmically computed decision are made and seek to scrutinise the outcome, this human final decision-making is far from being independent or even neutral. Human operators do not have the capability to independently assess the data-driven computed result. They are part of the security system and not at all independent from the algorithmic result. They can only compare the computed outcome with their own security assessment. Machines are, moreover, not more ethical than persons, given the potential human biases that are implemented in the machine's functioning. However, both assessments, the one of the human operator and the one of the data-driven algorithm, are based on different presumptions, different observations and finally different conclusions. Even knowing the functioning, problems and the fallibility of algorithmic profiling, security operators will hardly be able to break free from it and make an independent final decision (Matzner 2013). The question whether an "independent" decision is more adequate or even "better" than the algorithm based decision remains open.

The introduction of algorithmic profiling thus implies a set of accountability problems. Even in a system with a human final decision competence, it is hardly possible that human operators are entirely independent from data-driven influences. Thus, the responsibility for security decisions no longer lies exclusively with the human operator. The unclear distribution of responsibility between the security personnel and the data-driven routine – or rather its programmers – is inherent to the use of algorithmic profiling. This is especially problematic in situations when individuals want to challenge concrete security decisions. Even if the interviewed state authorities and data protection authorities insist on a human final decision competence (Interview 2, l. 872–77; Interview 6, l. 482–88; Interview 7, l. 130–34), the accountability problems persist. The idea of an entirely independent human final

decision thus turns out to be an illusion. The problem of the distribution of accountability directly affects the possibility to effectively challenge security decisions and needs to be scrutinised in the further development of airport security. Regarding the results of the conducted interviews, it seems to be necessary to raise awareness of this problem.

5.2 Problem Awareness

By describing some ethical problems that arise from the usage of algorithmic decision-making and big data, we wanted to see, which of these problems – if any – the proponents and the representatives from data protection agencies and NGOs identify.

As shown already by several quotes, most of the questions about possible and probable problems and challenges such as discrimination, unfairness, wrong data and wrong conclusions were either answered by referring to the very early stage at which smart security initiatives still are or by referring to regulatory and government bodies that are supposed to be in charge of these issues. Nevertheless, the lobbying for the introduction of these measures is ongoing although the problems are neither assessed nor tackled – if that is possible at all. Interestingly, interviewees are lobbying for data-driven risk assessment even after admitting the sensitivity of the data issue that kept them from progressing over the last couple of years (Interview 4, l. 284–85). In the following, we will present some of the (possible) problems that were mentioned either by data protection agency representatives or NGO representatives.

Identified Problems

One problem that was raised several times by NGOs is that by collecting vast amounts of data, sensitive data might also be part of the data base and allow for discrimination. Additionally, even if data is not obviously classified as sensitive, it might reveal a lot more about a person's private life, especially when compared and related to other data items (Interview 8, l. 535–49). Some proponents of smart security showed a limited awareness of the problems of sensitive data (e.g. Interview 4, l. 284–85; Interview 7, l. 59–64), others said there was no discussion about it or even showed – by naming an extensive amount of possible data sources, such as political memberships, Facebook profiles etc. – that in fact, there is no awareness of problems arising from large and widespread data collection (Interviews 1 and 5). However, German state representatives highlighted there should be no collection of vast amounts of data. They also referred to a poll taken among international passengers travelling through Germany, which showed that a large majority of travellers is quite satisfied with the security screening process. They accept that there have to be security checks that take some time, and when asked if they would prefer to reveal some information about themselves such as a known traveller programme would require, a majority of more than 80% opted for a security screening that might take more time but works without having to hand over personal data (Interview 6, l. 697–738).

Another requirement for data-driven profiling was brought to the fore by interviewees regarding the safe storage of the data (Interview 2, l. 1467–48), the guaranteed deletion of data (Interview 3, l. 502) as well as the general problems that arise out of a data collection such as possible misuse of data and ways of surveillance (Interview 8, l. 208–11). One

interviewee stated that we cannot be sure to live in a democratic state forever and nobody knows for what purpose these databases may be used later (Interview 8, l. 504–06). In fact, not taking into account the social costs of the data collection was criticised (Interview 8, l. 769). We only noticed some kind of awareness of these issues by the interviewees with a state bureaucracy background who do not want to collect more data because of the problems that this entails (however, the problem of misuse is not seen to the same extent [Interview 6, l. 650–52]). Interviewees supporting data-driven smart security did not recognise such problems; one interviewee even stated that we all knew that there was no privacy anymore (Interview 5, l. 95) which is why more data collection would not hurt.

Especially NGOs working in the field of privacy demand for safeguards regarding the collection and storage as well as for the usage and analysis of data. Here, transparency of the whole decision process and effective control of the data usage was demanded (Interview 3, l. 525–32). This is important as data-driven risk assessment 'derives assumptions of reality out of statistical correlations' (Interview 2, l. 706–07). From a legal point of view, citizens need to be given a clear idea of which behaviour triggers which reaction by the state. Citizens need to be able to assess the decisions that a state representative takes and has the right to a transparent decision process (Interview 2, l. 667–75). In Germany for instance, there is a general right to information on what the state authorities know about oneself unless there is an ongoing criminal investigation (Interview 8, l. 980). This does also apply to security data bases as ruled by the Federal Constitutional Court (Interview 2, l. 585–87).

There is no thorough understanding of these requirements when talking about smart security. Some interviewees said that not even security officials should have insights into the algorithmic decision-making process as discussed in the prior section on accountability. Some proponents, however, stated there should be at least some transparency for the passengers and they should be able to have 'access to some information' (Interview 5, l. 973). Also, the involved security personnel should be able to understand, scrutinise and also challenge how the decision-making algorithms work: 'So if we have a differentiated screening-approach, you should be able to go through the data afterwards, and say, well, this person was screened as low risk for this and this reason.' (Interview 4, l. 782–83, see also Interview 5, l. 980–81; Interview 2, l. 872–77). There is a demand for a transparent process of algorithmic decision-making. However, how this could or should be implemented technically when using self-learning algorithms was not thematised. In fact, it is nearly impossible to trace back such decisions and at the same time keep the algorithm secret and the unpredictability high – which is also demanded by proponents of smart security (Interview 1, l. 487–88).

Resistance

Another important point to examine is the possibility to resist against smart security decisions. In this context, resistance means the possibility of challenging and correcting wrong conclusions from given data. Here, we observed that this is something that is demanded by all NGO and data protection representatives we talked to and all proponents of smart security: The ability to challenge wrong data and/or wrong conclusions. All interviewees share the opinion that algorithms alone are not to be trusted. NGO representatives stated that data-driven decision-making is still very error-prone, which has real and problematic consequences (Interview 3, l. 521–25; Interview 8, l. 188–90) and a practitioner said that 'a kind of appeals-type of process […] would be logical to have'

(Interview 1, l. 356–57). Data protection experts added that there is a protective goal called "intervenability" which requires the actual chance to understand and challenge decisions taken by state actors (Interview 2, l. 766–70).

When we asked representatives from the aviation sector what this "actual chance" could look like, we heard that there was 'no discussion on this so far' (Interview 5, l. 1019) or the topic was changed very quickly (Interview 1, l. 356–64). As discussed in the section on accountability, some see a solution in a human officer being involved in the last decision. This, however, clearly does not solve the problem due to a lack of transparency, the seemingly objective character of computer-based decisions and the inability of human operators to act independently.

It is astonishing that although all interview partners share basically the same opinion on the critical issue of challenging wrong data and wrong conclusions, there is no theoretical, nor a practical approach. However, the lobbying for the introduction of the decision-making algorithms in question is ongoing.

On the other hand, we also realised from our research when talking to NGOs and data protection experts that there was an awareness of human rights problems of risk assessment and data collection in general. However, there was very little information or awareness on what is planned and already worked on in smart security initiatives. One representative admitted that there is hardly any NGO dealing with this (Interview 3, l. 758). This is most likely due to the opaque developing process of smart security which prevents a broad public debate as well as the in-depth engagement of actors from the civil society.

6. Conclusions: How Smart Is "Smart Security" and How much Security Is in "Smart Security"?

The development of smart security initiatives appears to be in the early stage. However, as most endeavours are hardly older than five years, proponents of smart security have made remarkable progress in many fields of implementation. To answer the question 'How smart is smart security?' different points need to be considered:

Smart Security Assemblage

Smart security consists of various elements. A more intelligent lane design, explosive trace detection, centralised image processing, body scanners, behaviour analysis and individualised risk assessment are just a few security routines that belong to smart security as an umbrella term. While some, like centralised image processing or an improved lane design are rather uncritical from a human rights point of view, others need to be scrutinised. In our report, we focused on the evaluation of individualised risk assessment and thus of the deployment of data-driven profiling.

Current lobbying rather appears to aim at implementing voluntary programmes which are comparable to the US-based TSA PreCheck. These programmes, better known as known traveller programmes, are one pillar of the strategy to foster the implementation of smart security at airports. The second pillar is the establishment of new smart security technologies, like body scanners or the centralised image processing. These systems are rather self-contained and not per se dependent on an external data support. However, they could also be elements of data-driven security routines that, if combined, would lead to a comprehensive data-driven and individualised security check. If, as stated, known traveller programmes ought to initiate a mind shift towards a broader acceptance of data-driven smart security, lobby efforts for them would mean the introduction of data-driven profiling through the backdoor. This is particularly problematic, as many problems linked to smart security have not been settled at all.

This report focused on the human rights implications of the establishment of data-driven profiling under the use of Big Data. In the process of our research, it has become quite obvious that especially problems connected to privacy issues and especially to the resistance against algorithmic security decisions have not been satisfactorily addressed. There is no effective complaints management procedure envisaged at all. It remains furthermore unclear, how the misuse of data is to be prevented, which data sources should be used and how discrimination could be avoided. It remains thus opaque how a passenger might influence his/her respective "data double".

Discrimination

Secondly, the problem of discrimination seems to be inherent to the probabilistic allocation of passengers to different risk categories. Deductive rules based procedures might be at least slightly more transparent then inductive routines. However, given the unlikely availability

of the deductive rules and the general use of personal data, both remain problematic. Current legal privacy safeguards function in a static manner and thus fail to effectively counter the problems linked to the dynamic data-driven profiling. Due to the opaqueness of the development process of smart security, neither our interview partners from state bureaucracies nor from civil society have been comprehensively aware of the complications arising out of the deployment of data-driven smart security routines. In other technological processes, both are central controlling bodies that aim at ensuring a high level of compliance to human rights standards. Furthermore, the fuzzy distribution of accountability contributes to the impossibility of effectively issuing and processing an appeal. Thus the discrimination linked to the design of risk categories, the blurred distribution of accountability, the potential misuse of data and the shortcomings of existing human rights safeguards need to be brought on the table in order to get a better idea of the consequences of smart security.

How much security is in "Smart Security"?

The third point is that smart security promises to improve aviation security through individual risk assessment by simultaneously providing a better travel experience and reducing the costs for the industry. Smart security aims at replacing the "one size fits all" security screening with custom-tailored individual security assessments. While false negatives (i.e. not detected threats) are worst in aviation security, it appears rather unintuitive why probabilistic security hypotheses created by data-driven algorithms should increase the level of security by replacing an overall high-standard security screening. Data-driven smart security does not contribute to a higher security standard. It rather creates privacy issues through the use of large amounts of data while not satisfactorily resolving the human rights concerns described before. On the contrary, a comprehensive standardised security procedure would ensure both an overall high level of security and an at least more equal treatment of all passengers. Although 'there remains a substantial preference for more, rather than less equality within society' (Gandy 2010, 37), smart security differentiates passengers according to personal data and thus causes more inequality.

It seems more plausible that smart security aims at reducing security costs for the aviation industry. Smart security devices are designed to increase the throughput per lane and thus to reduce the security costs per passenger. Albeit cost efficiency is a legitimate goal for industry associations, it should not be realised at the expenses of the passengers' human rights (e.g. art. 13 of the Universal Declaration of Human Rights). According to our interview partners, unpredictability is a key feature to ensure a high level of security. Consequently, even if cost efficiency is to be considered as a factor in aviation security, this should be realised through the deployment of random routines with an appropriate baseline level and not through the collection of passengers' data.

Smart security initiatives embrace some approaches that are capable of increasing the level of airport security. Those approaches (e.g. central image processing, explosive trace detection) could be termed smart. Data-driven profiling, however, is in the early development stage. Although central questions concerning the concrete functioning have not yet been resolved, it turned out that data driven smart security is not likely to improve airport security. It is rather a means to increase cost efficiency. This, in turn, would affect the whole justification structure of smart security. That is why the central question of smart security initiatives is not "How smart is 'Smart Security'?" but "*How much security is in 'Smart Security'?*"

7. Policy Gaps and Policy Recommendations

The evolution and implementation of smart security initiatives entails some potential benefits, but also challenges and problems. In this chapter, we want to address policy gaps in order to develop policy recommendations for decision-makers as well as for other stakeholders involved in the field of smart security.

During our research for this project, we identified six central policy gaps that need to be addressed. The policy gaps are meant to be thought-provoking issues for decision-makers in state bureaucracies as well as for civil-societal actors and stakeholders in industry associations involved in the development of smart security initiatives.

1. Why and how should smart security routines be implemented?

The introduction of smart security initiatives is not an end in itself. Their usefulness rather depends on the improvements and benefits they entail. It was claimed that smart security technologies might increase the level of security while generating a better travel experience for those passengers that are considered to be of low risk. However, most interviewees stated unanimously and independent of their respective backgrounds that the deployment of randomness as a security element would also enhance the level of security. It might thus be unpredictability that makes the difference in security routines. The interviewed representatives of state bureaucracies were rather sceptical about the use of data-driven profiling. In contrast, the merits of a “one size fits all" approach like equal treatment and a constant high level of security were emphasised.

It is far from evident that there is a need for increased security routines at all. As long as smart security devices, like data-driven profiling, collect data in order to make a differentiated risk assessment, there is a strong need for justification of these practices with regards to the privacy of passengers and potential problems of discrimination, misuse and basic justice. Smart security initiatives thus have to make their goals in terms of cost efficiency, security or comfort open to discussion and compare them with alternative security solutions.

While the “one size fits all” approach could ensure a general high level of security, the use of randomly altering security intensities might reduce the costs for the airports and airlines alike. Cost efficiency is certainly a legitimate argument for economic actors. For regulators on all political levels, however, human rights and security issues should be paramount and not outweighed by economic reasoning.

Recommendation: The need for a higher level of security has to be proven before introducing new security devices and/or methods. Once the demand for temporally and spatially limited higher security is democratically assessed, regulators should opt for the alternative that entails the least disadvantages while sustaining a sound level of security. From today's point of view, this would be a comprehensive and standardised security check, equal for every passenger as it entails the least social disadvantages while providing high security. Considering economic factors like cost efficiency, first of all, we recommend that there should not be a price tag put on human rights and non-discrimination. Therefore, randomly adjusted intensities for security controls seem to be preferable to opaque data-driven routines due to privacy considerations, possible discrimination and misuse of information.

2. What is lobbyism for smart security aiming at?

Many stakeholders in the area are engaged in lobbyism on the European as well as on the national level. This includes industry representatives, public institutions from the member states and actors of the civil society. As it turned out that most European countries are reluctant to introduce data-driven security routines, the implementation of algorithmic profiling proceeds rather slowly. That is why industry involved in aviation security has shifted its lobbying approaches towards the establishment of known traveller programmes which would work on the basis of voluntarily provided data. Simultaneously, smart security devices, like body scanners or central image processing, are in the process of being developed. The evaluation of these lobby activities is twofold:

Firstly, the implementation of a known traveller programme is not as unproblematic as it may seem at first glance. It might, as industry representatives hope, foster a mind shift towards data-driven profiling. However, participants in the known traveller programme must know what their data is used for and what consequences this might entail for them. Without ensuring a high awareness level, the introduction of known traveller programmes is ethically highly problematic. Before the backdrop of human rights standards, regulators need to consider awareness as well as general privacy issues before supporting a known traveller programme. Regulators, thus, need to clarify how a known traveller programme is planned to be used, with whom data is shared and to which end it is implemented.

Secondly, the development of new security routines requires a differentiated assessment. Some routines, like the design of security lanes, explosive trace detection and central image processing are capable of increasing the throughput of security checks while simultaneously enhancing the level of security. However, these smart security devices are self-contained and do not need to be supplied with passengers' data, so that passenger-awareness-issues do not arise. Other security devices, like behaviour analysis, are posing particular human rights problems which need to be further examined.

The USA, in contrast to Europe, have already introduced risk-based security systems. However, the known traveller programme "PreCheck" (run by the TSA) is falling short of expectations. That is one reason why, according to our interviews, the US authorities plan to conduct a survey on the acceptance of data-driven programmes. Another poll in Germany

has also shown that aircraft passengers are sceptical about the introduction of data-demanding programmes.

> **Recommendation:** European as well as national authorities should be aware of lobbying strategies of the aviation industry. Known traveller programmes might initiate a mind shift towards an increased acceptance of data-driven profiling. However, public acceptance is not to be confused with ethical acceptability. Thus, human rights issues in general and privacy issues in particular need to be thoroughly reflected and protected before permitting data-driven profiling. For this sake, regulators should invite pro-actively all stakeholders in the field of aviation security, including human rights actors in order to be able to consider a broad range of perspectives on the topic.

3. What data sources should (not) be used for smart security and how are passengers to be allocated to pre-defined categories?

Data-driven profiling relies on the use of a wide range of data, including data from social media, voluntarily supplied data and potentially also governmental data. All these categories embrace a set of particularly sensitive data (e.g. data concerning religion, race, sexuality, political membership). While at least some interviewees have shown a certain level of awareness of the problems connected to the use of sensitive data, the considerations concerning data protection and privacy issues are, optimistically spoken, in the early stages. It is crucial to develop robust data protection mechanisms that also guarantee the disuse of sensitive data.

Even if voluntarily provided data might be used for data-driven profiling in the context of e.g. known traveller programmes, interviewees especially from data protection authorities stated that they must only be used for the particular purpose for which they were provided to airlines and/or airports. A wider use or the transfer of the data needs to be prevented by strict data protection regulations.

The allocation of passengers to pre-defined categories necessarily entails a certain level of either positive or negative discrimination. The design of the criteria leading to this allocation, thus, needs to be examined regarding their discriminatory potential. It is far from clear whether risk categories are to be shaped via identifying a low or a high risk category. Both alternatives bear certain problems: Creating a special low risk category reduces the security checks for the individuals subsumed under this category. As this categorisation is always just a security hypothesis, an increase in false negatives might be the result. However, false negatives are probably the worst that can happen in the aviation sector. Consequently, low risk categories do not help to increase the overall level of security, but only decrease the security costs for the aviation industry.

The creation of high risk categories, on the contrary, entails the risk of discrimination and finally of severe disadvantages (including potential no-board lists) for the affected passengers. High risk categories are, like risk categories in general, created on the basis of data analysis and/or deductive risk assumptions. While those assumptions always reveal a certain perspective on the world, inductive data analysis might be subject to a certain selection bias and always compares behaviour to a certain "normal" and expected behaviour, thereby discriminating people at the boundaries of our societies

Recommendation: It has to be ensured that sensitive passenger data and the evaluation of a passenger's way of life are not in the focus of data collection. Once identified, sensitive data items must be deleted from databases. It needs to be taken into account that many kinds of data that are not considered sensitive in the first place, might become sensitive due a combination of several data sources. Furthermore, voluntarily given data must only be used with regard to the purpose of their collection. The transfer and the hidden use of the data must be prevented in order to meet privacy- and thus human rights standards. As the design of risk categories is inherently problematic, proponents of data-driven profiling must argue why its application is nevertheless justified in specific cases for which it can be shown that: a) how risk categories increase the overall level of security while avoiding any discrimination of passengers; and b) why personal risk assessment is an advantage in terms of security compared to non-discriminatory, standardised and equal security checks.

4. What measures are undertaken to counter the misuse of data?

The collection of data always entails the probability of misuse. Although it is crucial to develop safeguards for data-protection, there is only a limited level of awareness on the side of smart security proponents. Data collection, data storage and data processing demand a high level of problem awareness and a robust data protection concept. In the absence of the two, data-driven security poses a threat to passengers' privacy. However, individual human rights like the right to freedom of personal development must not be jeopardised for the introduction of data-driven profiling.

Recommendation: European and national regulators need to make sure that privacy issues are considered in aviation security. The inherent risk of misuse of data needs to be taken into account for a comprehensive evaluation of data-driven security routines. A convincing privacy concept that entails effective safeguards should thus be a precondition for further negotiations on the introduction of data-driven security routines.

5. Who is accountable for security decisions in the end?

Data-driven profiling results in computed risk assessments that lead to security decisions with real life consequences. Albeit those decisions are executed by human operators, security personnel in a data-driven security environment act on the basis of algorithmic routines. Many interviewees considered uninformed human operators as an advantage in terms of neutral and unbiased security decisions. This, in turn, means that security personnel are hardly able to challenge flawed algorithmic assessments. Even well-trained operators remain part of a combined algorithmic-human security check and thus biased by the computed outcome.

Human operators cannot exclusively be held responsible for a data-driven security decision. But on the other side, accountability gets fuzzy when applied to algorithms. The idea of an independent human final decision is thus rather naïve.

A clear-cut allocation of responsibility is almost impossible under the condition of data-driven security. This problem gets even bigger when it comes to inductively working, fluid data-driven security routines. Accountability, however, is a key feature for effective human rights safeguards. While existing privacy safeguards act in a static fashion, depending on privacy legislation, data-driven routines act on a dynamic basis. This renders the present safeguards inappropriate for a comprehensive level of human rights protection.

Recommendation: A clear-cut concept of accountability ought to be a criterion for the introduction of smart security routines. The advantages and disadvantages linked to the employment of uninformed human operators need to be further analysed. Prior to the implementation of data-driven routines, it needs to be examined how human rights safeguards are to be altered in order to provide an effective human rights protection.

6. How could appeals against security decisions be a part of smart security?

Although all interviewees unanimously expressed the need for standardised processes for challenging security decisions, there is hardly any concrete plan for how appeals might be dealt with in practice. As safeguards are rendered rather ineffective under the condition of data-driven security routines, there is no competent authority that might effectively support passengers' appeals against security decisions. As the investigation of an appeal would otherwise be up to the discretion of the operator of the algorithm, the establishment of an effectively working, independent authority that is able to assess passengers' appeals should be compulsory.

Recommendation: The possibility to challenge security decisions is crucial in terms of human rights standards. Thus, data-driven security must not override the right to effective appeal. As passengers might end up on a no-board list, regulators need to make sure that the affected passengers have legal means and ways to effectively challenge a particular decision. It needs furthermore to be guaranteed that these issued appeals are processed in an independent fashion. State bureaucracies need thus to make sure that security decisions can be made transparent for the treatment of appeals. Additionally, individuals should receive meaningful information about the logic involved in any automated processing and guidance on its interpretation by a counselling body in order to be in a position to challenge a particular decision. Given both the sensitivity of most data and the overall willingness of the involved actors to implement appeal mechanisms, it is the duty of the regulators to design appeals procedures that correspond to the safeguards' capabilities in order to finally ensure an independent appeal procedure that is subject to public supervision.

8. Need for Further Research

The report revealed the comprehensive state of the art with regard to problems of algorithmic profiling. However, the research on data-driven smart security routines is in a rather early stage. As long as the particular design of data-driven smart security routines remains opaque, only general implications of algorithmic security routines can be assessed. In order to get deeper insights into emerging security routines and compare their human rights implications with those of existing security practices, we identified four central fields for further research:

1. Existing security routines that do not depend on the use of Big Data need to be analysed with regard to their human rights implications.
2. The emerging field of behaviour analysis which might be combined with emotion recognition demands a higher awareness level including comprehensive research on affected ethical and human rights issues.
3. Before implementing data-driven security routines, comprehensive research has to be undertaken in order to identify how resistance might be possible under the condition of data-driven security routines. Moreover, it needs to be examined how such processes should be designed to work effectively.
4. Finally, the question of technologies that use differentiation and pattern building discriminate per se requires more attention. Therefore, it is necessary to conduct more fundamental research on the link between differentiation and discrimination.

Acknowledgements

We would like to thank Kirsten Fiedler (European Digital Rights, EDRi) and Chris Jones (Statewatch) for their helpful comments and remarks on an earlier version of this report.

We also thank our student assistants whose dedicated and thorough work contributed essentially to realising this report in time.

List of Abbreviations

ACI	Airport Council International
API	Advanced Passenger Information
CAPPS	Computer Assisted Passenger Pre-screening System
CIP	Centralised Image Processing
EU	European Union
IATA	International Air Transportation Association
PNR	Passenger Name Record
TSA	Transportation Security Administration

Bibliography

Adey P (2003) Secured and Sorted Mobilities: Examples from the Airport. Surveillance & Society 1(4): 500–19.

Adey P (2008) Mobilities and Modulations: The Airport as a Difference Machine. In Salter M B (ed.) Politics at the Airport. Minneapolis/London: University of Minnesota Press: 145–160.

Amoore L (2011) Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. Theory, Culture & Society 28(6): 24–43.

Bellanova R and González Fuster G (2013) Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices. International Political Sociology 7(2): 188–209.

Barkin S (2008) 'Qualitative' Methods? In Klotz A & Prakash D (eds.) Qualitative Methods in International Relations. A Pluralist Guide. Basingstoke: Palgrave Macmillan.

Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D and Walker R B J (2014) After Snowden: Rethinking the Impact of Surveillance. International Political Sociology 8(2): 121–44.

boyd d and Crawford K (2012) Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society 15(5): 662–79.

de Vries K (2010) Identity, Profiling Algorithms and a World of Ambient Intelligence. Ethics and Information Technology 12(1): 71–85.

Edel F (2010) The Prohibition of Discrimination Under the European Convention on Human Rights. Strasbourg: Council of Europe Publishing.

Foucault M (2007) Security, Territory, Population. Lectures at the Collège de France, 1977–78. New York: Palgrave Macmillan.

Foucault M (2008) The Birth of Biopolitics. Lectures at the Collège de France 1978–79. New York: Palgrave Macmillan.

Gandy O H (2010) Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems. Ethics and Information Technology 12(1): 29–42.

Gusterson H (2008) Ethnographic Research. In Klotz A & Prakash D (eds.) Qualitative Methods in International Relations. A Pluralist Guide. Basingstoke: Palgrave Macmillan.

Guzik K (2009) Discrimination by Design: Predictive Data Mining as Security Practice in the United States' 'War on Terror'. Surveillance & Society 7(1): 3–20.

Haggerty K D and Ericson R V (2000) The Surveillant Assemblage. British Journal of Sociology 51(4): 605–22.

Hobbing P (2010) Tracing Terrorists: The European Union-Canada Agreement on Passenger Name Record (PNR) Matters. In Salter M B (ed.) Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror. London/New York: Routledge: 73–97.

IATA (undated) Checkpoint of the Future. Executive Summary, IATA report.

IATA/ACI (undated a) Smart Security, IATA and ACI leaflet.

IATA/ACI (undated b) Smart Security. Smart Security Module Passenger screening, IATA and ACI leaflet.

IATA/ACU (undated c) Smart Security. Smart Security Module Centralized Image Processing, IATA and ACI leaflet.

IATA/ACU (undated d) Smart Security. Smart Security Module Behaviour Analysis, IATA and ACI leaflet.

Leese M (2013) Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs. Computer Law & Security Review 29(5): 480–90.

Leese M (2014) The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union. Security Dialogue 45(5): 494–511.

Leese M and Koenigseder A (2015) Humor at the Airport? Visualization, Exposure, and Laughter in the "War on Terror". International Political Sociology 9(1): 37–52.

Lyon D (2003a) Airports as Data Filters: Converging Surveillance Systems after September 11th. Journal of Information, Communication and Ethics in Society 1(1): 13–20.

Lyon D (ed.) 2003b. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, London/New York: Routledge.

Lyon D (2006) Surveillance, Security and Social Sorting: Emerging Research Priorities. International Criminal Justice Review (17)3: 161–70.

Kevin Macnish (2012) Unblinking Eyes: The Ethics of Automating Surveillance. Ethics and Information Technology 14(2): 151–67.

Maguire M (2014) Counter-Terrorism in European Airports. In Maguire M, Frois C, and Zurawski N (eds.) The Anthropology of Security: Perspectives from the Frontline of Policing, Counter-Terrorism and Border Control, London and New York: Pluto Books.

Matzner T (2013) The Model Gap: Cognitive Systems in Security Applications and Their Ethical Implications. AI & Society online first: 10.1007/s00146-013-0525-4.

Matzner T (2014) Why Privacy is not Enough Privacy in the Context of "Ubiquitous Computing" and "Big Data". Journal of Information, Communication and Ethics in Society 12(2): 93–106.

Muller B J (2010) Unsafe at any Speed? Borders, Mobility and 'Safe Citizenship'. Citizenship Studies 14(1): 75–88.

Rosch P (2014) Checkpoint of the Future? – Von der klassischen Gefahrenabwehr zur modernen Gefahrenvorsorge in der Luftsicherheit. In Wagner K and Bonß W (eds.): Risikobasiert versus One Size Fits All: Neue Konzepte der Passagierüberprüfung im Luftverkehr, SIRA (3): 57-72.

Rouvroy A (2013) The End(s) of Critique: Data-behaviourism vs. Due-process. In Hildebrandt M & de Vries K (eds.) Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology. Milton Park/New York: Routledge: 143–68.

Salter M B (2008a) Imagining Numbers: Risk, Quantification, and Aviation Security. Security Dialogue 39(2–3): 243–66.

Salter M B (ed.) 2008b. Politics at the Airport, Minneapolis/London: University of Minnesota Press.

Valkenburg G and van der Ploeg I (2015) Materialities Between Security and Privacy: A Constructivist Account of Airport Security Scanners. Security Dialogue 46(4): 326–44.

Vermeulen M and Bellanova R (2012) European 'Smart' Surveillance: What's at Stake for Data Protection, Privacy and Non-discrimination? Security & Human Rights 23(4): 297–311.

Virilio P (1997) The Overexposed City. In Leach N (ed.): Rethinking Architecture: a Reader in Cultural Theory, London: Routledge: 381–90.

Zukowsky J (1996) Introduction. In Zukowsky J (ed.) Building for Air Travel: Architecture and design for commercial aviation, New York: The Art Institute of Chicago/Prestel Verlag: 13–25.