universität wien

MASTERARBEIT

Titel der Masterarbeit

FIXING THE BODY SCANNER

A discursive Stakeholder Analysis of ATR Software in the United States of America

Verfasser

Reiner Kapeller, Bakk. phil.

angestrebter akademischer Grad

Master of Arts (MA)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 066 906
Studienrichtung lt. Studienblatt:	Masterstudium Science-Technology-Society
Betreuerin:	Mag. Dr. Katja Mayer

Acronyms

AIT – Advanced Imaging Technology

ATR – Automated Target Recognition

TSA – Transportation Security Agency

EPIC – Electronic Privacy Information Centre

STS – Science, Technology, Society

US – United States of America

SD – Stakeholder Documents

1. Introduction

> "Advanced imaging technology is one of the best layers of security we have to address the threats of today and tomorrow," said TSA Administrator John S. Pistole. "We remain committed to deploying this integral counterterrorism tool in order to ensure the highest level of security for the traveling public." … ATR is designed to enhance security by safely screening passengers for metallic and non-metallic threats—including weapons, explosives and other objects concealed under layers of clothing. (TSA, 2011: SD 5)

Every time a new technology leaves the testing phase to enter into service it is discussed, welcomed and contested by various stakeholders who assess the implications of the particular technology. Advanced Imaging Technology (AIT) has been in test use at airports since 2007. However, permission to introduce AIT on a larger scale was granted in December 2009, when the thwarted terrorist attack on Northwest Airlines Flight 253 raised political support for implementing AIT as a means to answer new threats. On that occasion, in an attempt to smuggle plastic explosives on board, Umar Farouk Abdulmutallab bypassed security controls that relied on detection through metal detectors. As a result, proponents of AIT claimed that the scanners would have been able to detect the explosive, which would have resulted in Abdulmutallab being prevented from boarding the plane in first place. AIT is set to replace metal detectors, which have been standard for passenger security controls at airports since the 1970s. The device works by emitting electromagnetic waves that bounce off the body surface and create a detailed picture of the passenger's skin surface. While public stakeholders, most prominently the news media and NGOs have criticized the invasive nature of taking so-called “naked images” of passengers (Tirosh & Birnhack, 2013), an Automated Target Recognition (ATR) software update has been released by the Transportation Security Administration (TSA) in 2011 to mitigate privacy concerns. ATR not only brings significant changes to the appearance of the scanners but also alters functionality of the technology. Whereas previously the reading of the passenger’s body surface relied on a remotely located TSA officer, ATR takes over the detection job. The software independently decides whose body poses a potential threat to airport security and whose body is harmless and can thus pass security controls. While the update has implications for the security process and passenger experiences at checkpoints, ATR software is also accompanied by rhetorical efforts to restore passenger confidence in AIT devices and the TSA as the responsible agency for providing security at airports. Hence, ATR software represents a second chance for the TSA to modify the perception of a technology that many

have already denounced as “porno-scanners” (Gillmor, 2010). While ATR is based on the AIT, the software is discursively reconstructed as an improvement over earlier practices by the TSA. Nevertheless, opponents of the technology criticize it just as much as AIT.

This thesis aims to follow the construction of discursive traces in stakeholder documents and the formulation of a manufactured reality that can be observed through words and patterns of talk. While discourses sometimes agree on general concepts (such as the welcomed feature of ATR software that obscures individual pictures of passengers by using a generic outline), Fairclough (2001) points out that particularly divergent discourses are a sign of ongoing social conflict. This thesis features US stakeholder documents, among them newspaper articles as well as official documents from the TSA and the Electronic Privacy Information Center (EPIC). Additionally, public commentaries from regulations.gov are taken into account to depict the multilayered conceptions of how security and privacy are perceived and discursively realized by various stakeholders in the debate over ATR software.

The theoretical part of this thesis consists of several subchapters. Chapter 2.1 (p. 25) reflects on current themes in the area of surveillance and media studies, while chapter 2.2 (p. 29) introduces the main surveillance theories that build the ground for the deliberations of this thesis. A theoretical discussion of ATR software is then undertaken using four main approaches. First, chapter 2.3 (p. 31) highlights the history of the human body as a source of identification that continues to play an important role in present-day detection and verification processes. Second, chapter 2.4 (p. 34) investigates the role of mechanical objectivity, which represents the core capability of ATR software to make autonomous decisions but at the same time also comes with implications for the work of the remaining TSA officer. Third, the visual alterations introduced by the software are then encountered via a theoretical approach to the practice of seeing in chapter 2.5 (p. 38). Finally, chapter 2.6 (p. 41) deals with privacy claims and concerns that are related to the depiction of the (naked) body, which becomes the center of attempts to balance sheer contradictory approaches of privacy and security.

The next major chapter introduces the research field, (p. 47) which highlights the stakeholders whose documents provide the foundation for the present discourse analysis. While the reader obtains information on the individual background of every stakeholder, this chapter also refers to alternative actors who have been excluded from the research for different reasons. Subsequently, the methods section introduces discourse analysis (p. 56) as well as qualitative content analysis (p. 58) and reflects on deliberations on combining the approaches accordingly (p. 59). Furthermore, this chapter will explain the interval of the data gathering period (p. 60) as well as general data access (p. 60) and a detailed explanation of

data collection (p. 61). Additionally, the main tool for the document analysis will be introduced (p. 63), while the last subchapter deals with reflections on data interpretation (p. 64).

The empirical part of this thesis deals with documents in which different stakeholders voice different opinions when engaged with ATR software. It is divided into three parts: (1) anomalies and detection through ATR software; (2) human-machine interaction and the perception of privacy; and (3) generic outline and the display of the human body. These categories are explained in greater detail below:

(1) Anomalies and detection through ATR software: As a consequence of the software update, detection is transferred from a human officer to a machine. This transfer implies a strong trust in technology: it holds the detection ability of scanners to be superior to that of a human. Here the notion of anomaly plays a key role as it conceives the software's ability to detect. Concerned with discourses of detection, this opens up the question of how ATR software is discursively rendered in connection to aviation threats, while also shedding light on the role of the body as it is transformed into a "machine-readable identifier" (van der Ploeg, 1999).

(2): Human-machine interaction and the perception of privacy: This chapter deals with the replacement of human workforce with ATR software. Following privacy concerns raised by passengers and the media, ATR software has been presented as having improved privacy standards as it foregoes the employment of a second TSA officer responsible for examining pictures of passengers, as was the case with AIT images. Furthermore, what was previously an interaction between two TSA officers is now a communication only between the ATR software and the officer responsible for verification of a potential threat. Besides discursive alterations to privacy, this transformation also contributes to perceptions of the work of TSA officers.

(3) Generic outline and the display of the human body: The third chapter examines discourses on the visual impact of ATR on stakeholders. The display of a generic outline represents the most visible alteration to the software and plays a key role in the perception of the scanners. Again, stakeholders discursively express perceptions about the importance and constitution of the concept of privacy and its relation to the visible body. Tracing the discourses will also shed light on whether unobtrusive measures such as the filter of a generic outline affect public perception of ATR software.

Following the empirical part of this thesis, a discussion and results section (p. 106) summarizes the observations made and seeks to reflect on the situation of the human body inside AIT devices. Additionally, an overview of future scenarios in which AIT can and will be used is provided. In summary, this work aims to consider several questions, of which the

following are the most critical: What happens to the individual body when it becomes the center of attention of surveillance technologies? How do stakeholders portray the detection ability of ATR software? What are the implications for TSA officers as they respond to instructions of a machine? In how far does concealment of the individual passenger affect conceptions of privacy? This thesis attempts to follow, compare, and analyze discourses that deal with the application of ATR software and to reach conclusions that will shed some light on how surveillance technology is affecting and transforming perceptions of privacy and security.

1.1. 9/11 and its aftermath

In the aftermath of the September 11th attacks in the United States, a number of significant changes occurred in the realm of surveillance and security. Indeed, authors such as Didier Bigo have described the post-9/11 landscape as a "permanent state of emergency" and a "generalized state of exception" (Bigo, 2006a). A fundamental feature of these states is said to be a specific form of governmentality of unease that increases the exception to a perpetual state that consequently banalizes it. Nevertheless, the impact of 9/11 cannot be conceived in terms of a never-before-seen event. Although many leading politicians of the time, including British prime minister Tony Blair and US president George W. Bush, portrayed 9/11 as a turning point in history (Huysmans, 2004), the political violence represented through terrorism builds upon a long history that never flinched from transcending national borders and has reappeared in regions all over the world. Beginning with the second half of the 20th century, terrorism has been characterized by such measures as the hijacking of aircraft, the killing of policemen, hostage taking, and the bombing of buildings (Roberts, 2006). Still, 9/11 changed the level of the use of violence as it combined many of the traditional tactics used by terrorists (hijacking aircrafts, destroying them, suicide bombers) but intensified the efforts of clandestine organizations by using technologically advanced weaponry (Bigo, 2006b: 50-51). However -- and this is Bigo's main point here -- the novelty of the September 11th attacks is not the type of terrorist conduct but rather the reactions of politicians responding to these shocks to society. As Bigo argues:

> "September 11 is not an exceptional event of violence which reframes the relations of politics; rather, it is the regression of some politicians towards the habits that reveal the logic of a form of governmentality which informs deeply what is called liberalism and generates illiberal practices" (ibid., 2006b: 51).

The domestic effects of 9/11 are now well-known: the enactment of Patriot Acts I and II and the major breaches of democracy seen through the use of military powers to try any aliens suspected of terrorism were brought to life by the Bush administration, which had declared "an extraordinary emergency" (ibid., 2006b: 51-52). In the aftermath of 9/11, the US popular sentiments of patriotism increased, as well as a desire for protection and a thirst for revenge. The achievement of hitting the undisputed global superpower right in its heart prompted feelings of great vulnerability, something mostly unfamiliar to the US. As in many instances in social history, the answer to this vulnerability has been sought in the form of certainty rooted in surveillance (Lyon, 2001) with the objective of minimizing potential risks. For a society that is concerned with the security of its citizens, risks require a constant evaluation and pro-

active legitimating of action to effectively minimize potential dangers (Ammicht & Rampp, 2009). This action has to be institutionalized and can most likely be achieved in areas featuring unique characteristics of high fluidity and vastly different visitor streams. As airports also serve as gates to nations, heightened vigilance permits the special characteristic of this place to continue.

1.1.1. The airport as a place

Whereas some called September 11th an exceptional event of “hyperterrorism”, Bigo (2006b) sees a series of destructive bombings from 9/11 to Madrid in March 2004 and London in 2005. In order to respond to the threat of terrorism, governments around the world have increased surveillance at hot spots with great streams of visitors. Many of these new security measures have been tested at airports. Consequently, the airport has been described in accordance with Michel Foucault (1975) as a place of extreme discipline, where privacy-invading security measures are more likely to be more accepted than elsewhere (Lyon, 2003: 13). Moreover, measures taken at the airport are also highly visible. Politicians can assure the public that they are responding to dangers by implementing high-tech solutions, and security companies are keen on portraying technology as an ideal tool for demanding situations. David Lyon has called airports “perhaps the most stringently surveilled sites in terms of the means of movement and identification” (Lyon, 2007: 123). With passengers coming from places all over the world airports represent vulnerable nodes and high-value targets in an incredibly complex framework of national and international security (Seidenstaat, 2004).

There is at least some ambiguity in the interpretability of the airport as a place. For many the airport serves as a departure point for freedom and dream vacation as well as a somehow familiar 'non-place' of consumption (Augé, 1995). Today’s airports face three major dilemmas and/or tasks in terms of providing airport security: Space, speed, and sharing. Security measures have to make due with limited space as well as with an ever-growing number of passengers that have to pass through security procedures as fast as possible so that flights can operate on time and airport customers have time to spend extra money on airport facilities such as restaurants, and duty-free shops. It is an interesting double contingency that lives within the airport. On the one hand, travelers are regarded as ever more important potential consumers, while on the other hand they remain a calculable threat risk. In both cases, the airport takes in the place of a “data filter” (Lyon, 2002c: 123): it is a place where airlines establish different classes of passengers and early boarding represents a distinctive

feature but also where governments enforce so-called 'no-fly' lists. The aims of today's airport are thus both to maximize but also regulate mobility (Salter, 2008: 34). Hence the role of security in particular has turned into a major concern for airports today. After all, security is not only an obligation, but it also accounts for great part of airport investments: "Security has become a key cost component in high risk organizations, especially in the area of air transportation. It is most visible in the aviation industry and accounts for about a little over one-quarter of airports operating costs" (Kirschenbaum, 2013). The day-to-day basis for handling security checks at airports has undergone various changes over time. Whereas security controls through the 1960s and 1970s focused on the threat of hijacking and screened individuals immediately before boarding the plane, the majority of the airport space remained for the public. However, as terrorist attacks increased, security screening moved away from the gates to centralized screening points (Salter, 2008: 13). Not only are security procedures at airports changing, but the different ways in which terrorists harm society have also become the focus of airport security. Plastic explosives amount to a relatively new danger, while metal detectors, widely used at current airport security checkpoints, rely on technology from the 1970s. Since that time, airport security in the US has come a long way. One of the latest efforts in providing airport security has come with the introduction of AIT to airport security controls. As we will see, the decision to implement this technology is related to a particular incident, namely the attempted terrorist attack by the infamous "Underwear Bomber".

1.1.1. Northwest Airlines Flight 253

When Umar Farouk Abdulmutallab boarded Northwest Airlines Flight 253 at Amsterdam's Schiphol Airport on Christmas Eve 2009 no one suspected the deadly threat the young man posed to fellow passengers:

> "On December 25, 2009, a 23-year-old Nigerian man, Umar Farouk Abdulmutallab attempted to detonate a concealed nonmetallic device containing the explosive pentaerythritol tetranitrate (PETN) on Northwest Airlines Flight 253 from Amsterdam to Detroit, Michigan, as the plane was descending into Detroit Metropolitan Wayne County Airport" (Select Committee on Intelligence United States Senate [SCOIUSS] 2010: 1).

Even though passengers on board where able to overwhelm Abdulmutallab while he was trying to ignite the explosive the incident led to discussions on intensifying security measures at airports worldwide. While image technology premiered in test use at Schiphol airport in 2007 (Brown, 2012), the thwarted terrorist attack has promoted image technology from being

a voluntary measure to a required one when flying to the US. Additional support for the decision was offered by the head of the Dutch Counter-Terrorism Agency: “We think that there is now a new threat, because of course this attack has been claimed by Al Qaeda. That’s why we take new measures and we introduce the body scan for the flights towards the United States” (Ter Horst, 2009). After the failed attack many other countries became interested in the installation of AIT, with the US calling for deployment as well. Former Secretary of Homeland Security Janet Napolitano argued: “By accelerating the deployment of this technology, we are enhancing our capability to detect and disrupt threats of terrorism across the nation” (Ahlers, 2010). Further support for the technology has come from Germany and other parts of the European Union, where the general consensus holds that the implementation of AIT could have prevented an attempted attack (Deutscher Bundestag [DB], 2010). Consequently, the near-occurrence of a terrorist attack helped AIT achieve a breakthrough and resulted in the introduction of the technology on a broad basis at US airports from 2009 on. While initial deployment of AIT had already begun in 2007 (Mironenko, 2011), the thwarted terrorist attack on Northwest Airlines Flight 253 prompted widespread distribution of the scanners. As AIT represents a relatively new security technology at airports, the following chapter will give an overview of the screening procedure and explain the basic concepts that passengers experience at security checkpoints.

1.2. Screening passengers

Today, AIT[1] scanners are ubiquitous at US airports. As a replacement for metal detectors, approximately 740 AIT units have been introduced at already 160 airports nationwide (TSA, 2013a), which accounts for almost half of the roughly 450 commercial airports in the US. The goal is to completely replace metal detectors in the future (Silverleib & Hunter, 2010). While the scanners are considerably larger than metal detectors the checkpoint looks largely the same and therefore retains a sense of familiarity. The main difference is that while with metal detectors had to walk through a portal or gate, AIT requires passengers to enter the scanner and stand still inside for a certain amount of time while imaging sensors rotate around the body to create a 360 degree picture (Congressional Research Service [CRS], 2012). The technology also requires passengers to raise their arms above their head so that AIT can

[1] AIT has been tagged with various descriptions naming Body Scanners, Whole-Body Imaging, Security Scanners, or Full Body Scanners only the most common. While these descriptions are of great importance for argumentations and characteristics in the present Discourse Analysis, the technology will be continuously named AIT outside of stakeholder documents and citations. This decision has been made to keep a clear separation between notions used by the stakeholders and a more neutral conception applied by the researcher. This is also an attempt by the researcher to avoid interference with the usage of popular terms that show a bias towards certain conceptions of the technology.

generate a picture of the human body that is free from obscured parts of the body as, for example, the armpit area. AIT screening is applicable for "anyone who can stand without a mobility aid, cane, crutches, walker, etc., for 5-7 seconds with their arms raised above shoulder level" (Walton, 2010). The use of AIT is technically voluntary. Passengers who don't want to be screened can choose an enhanced pat-down instead. This procedure (in this case by a female officer)

> "Will be performed by an officer of your gender. The officer will run a handheld metal-detecting wand over your, then run her hands across your body to feel for forbidden items such as weapons. You must tell the officer if you have any medical devices, such as pacemakers, before she begins the screening. Once the officer is satisfied that you're not carrying any contraband, she'll let you continue to the gate" (Walsh, 2010).

When passengers enter the screening area they encounter two signs that relate to AIT and indicate how the scanning process is executed. While Figure (1) describes the technology in plain terms, Figure (2) predominantly indicates that the use of the technology is optional.

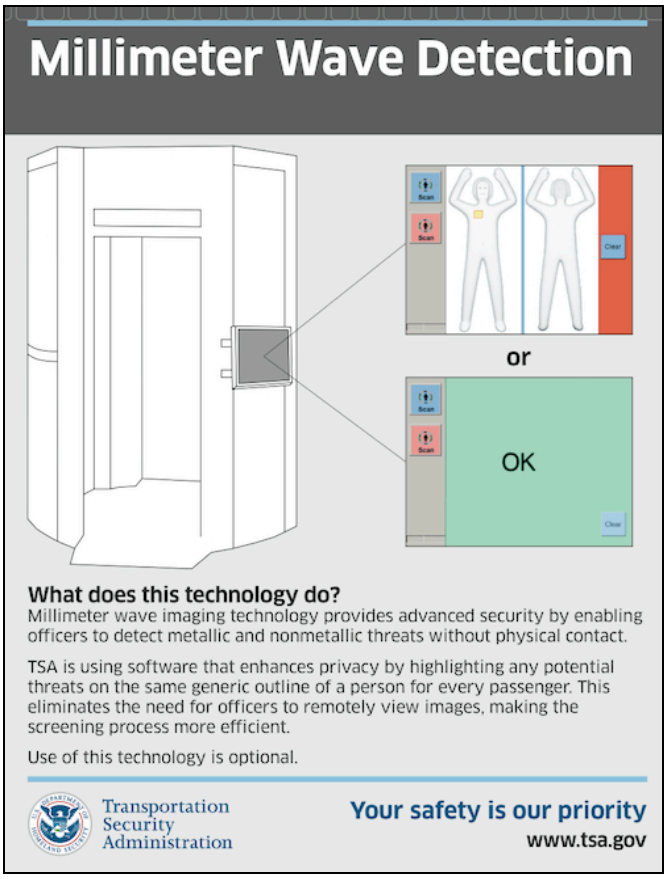

Figure (1): Millimeter Wave Detection Info

Figure (2): Millimeter-Wave Detection: Use of this technology is optional

1.2.1. Procedure of the screening process

The following description is taken directly from the TSA website (TSA, 2013b):

"Before going through this technology, remove ALL items from pockets and certain accessories, including wallet, belt, bulky jewellery, money, keys, and cell phone. Removing all of these items will reduce the chances of needing additional screening after exiting the machine. After everything is removed from pockets, passengers will be directed to walk into the imaging portal. Once inside, passengers will be asked to stand in a position and remain still for a few seconds while the technology creates an image of the passenger in real time. Advanced Imaging Technology Millimeter-Wave units use Automated Target Recognition, which eliminates passenger-specific images. Instead, the software automatically detects potential threat items and indicates their location on a generic outline of a person that will appear on a monitor attached to the unit.

The passenger then exits the opposite side of the portal and collects their belongings. The entire process takes less than one minute. To avoid the chance of leaving any personal

items behind, passengers are encouraged to place them in their carry-on bag prior to entering the checkpoint."

While the description above is largely concerned with the setting and the procedures that passengers experience at airports, the next chapter deals with two technology concepts that have defined AIT so far. While passengers today only encounter the type of AIT that uses millimeter wave technology, the history of AIT at airports appears to be more diverse.

1.3. Advanced Imaging Technology

After the thwarted terrorist attack of Northwest Airlines Flight 253, AIT was mentioned as a possible solution as it can detect non-metallic threats such as the explosives smuggled aboard of the plane, therefore making it a more vigilant technology than the commonly used metal detectors (Mironenko 2011: 233). According to a bill introduced to the US Senate in 2010 entitled Securing Aircraft From Explosives Responsibly: Advanced Imaging Recognition Act (S.A.F.E.R. A.I.R. Act), AIT can be understood as a device that creates a visual image of an individual person showing the surface of the skin and consequently revealing other objects on the body as applicable, including narcotics, explosives and other weapons components (ibid., 2011). The TSA has been using two types of scanning devices at airports that rely on different technology in terms of screening passengers. While the scanners use different technologies they nevertheless rely on the same technological principle of emitting waves onto the body and using the reflection to create a picture of an individual human. The first type of scanners is known as Backscatter[2] and the second works by relying on emitting millimeter waves[3].

[2] Backscatter (low X-Ray) technology is based on the X-Ray compton scattering effect. It detects the radiation reflected from the object to form a 2D image. Images are taken from both sides of the human body (Mironenko, 2011: 233).

[3] In this technology, clothing and other organic materials are translucent in extremely high frequency (millimeter wave) radio frequency bands. The millimeter waves are transmitted simultaneously from two antennas rotating around the body. The wave energy reflected back from the body or other objects on the body is then used to construct a three-dimensional image (ibid., 2011: 233).

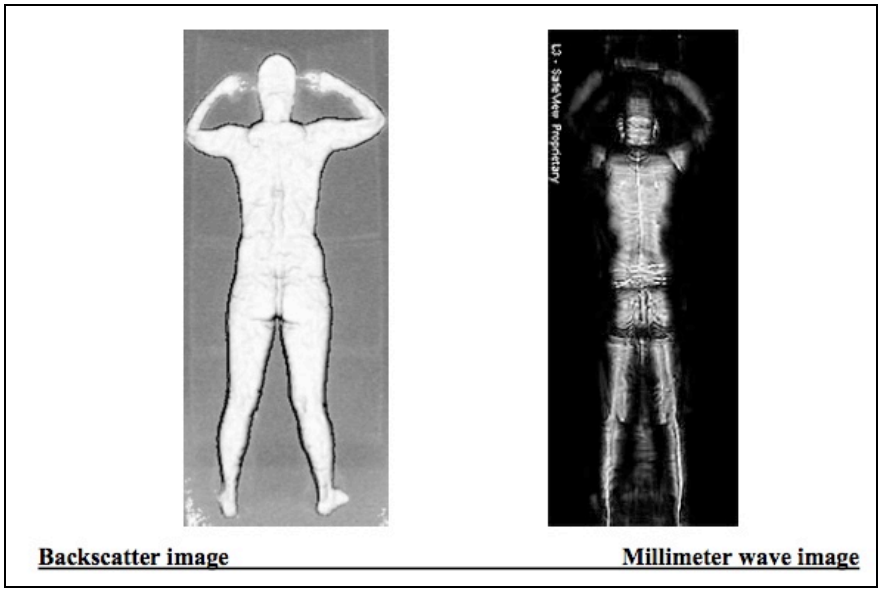

Figure (3): Sample image of Backscatter (X-Ray) and Millimeter-Wave Technology

In an embarrassing incident in November 2010, it was revealed that US marshals operating a millimeter-wave device in Orlando had stored some 35,000 photographs. One hundred of these pictures were published online, and the incident caused tremendous public disgust (Johnson, 2010). By then, terms such as “Naked Scanners” and “Virtual Strip Search” had already spread. The TSA emphasized that the ability to store images would not be included in the software of AIT devices placed at airports, and that there is no capability to activate image storage functions. Initial versions of AIT were manufactured with storage functions that had to be disabled prior to installation at the airport. According to the TSA, current versions of the software do not include any storage function at all (U.S. Department of Homeland Security [USDOHS], 2011). On July 2, 2010 the Electronic Privacy Information Center (EPIC) filed a lawsuit to stop the deployment of AIT at US airports. EPIC argued that use of the device violated the Administrative Procedures Act, the Privacy Act, the Religious Freedom Restoration Act, and the Fourth Amendment (EPIC, 2013a). Federal courts have acknowledged EPIC's criticism and the TSA has agreed – in the face of growing public protest – to remove Backscatter X-Ray devices from all US airports by June 1, 2013. The official reason for this move does not cite any potential health risks associated with the emission of x-rays. Instead, the TSA cited the inability of manufacturer Rapiscan to come up with an ATR solution for their Backscatter devices in a timely manner (Burns, 2013a). As a consequence, millimeter-wave technology has replaced all Backscatter devices at US airports. This systematic move by the TSA to dismiss the great base of Backscatter scanners also demonstrates the overall importance of ATR software for the agency's reputation.

1.4. Automated target recognition

ATR is a software that replaces the current image of the human body with a generic outline, comparable to a stick figure (USDOHS, 2011). So as to assuage privacy concerns the photograph is turned automatically into a much more friendly cartoon-like outline that doesn't generate as much uproar as previous pictures.

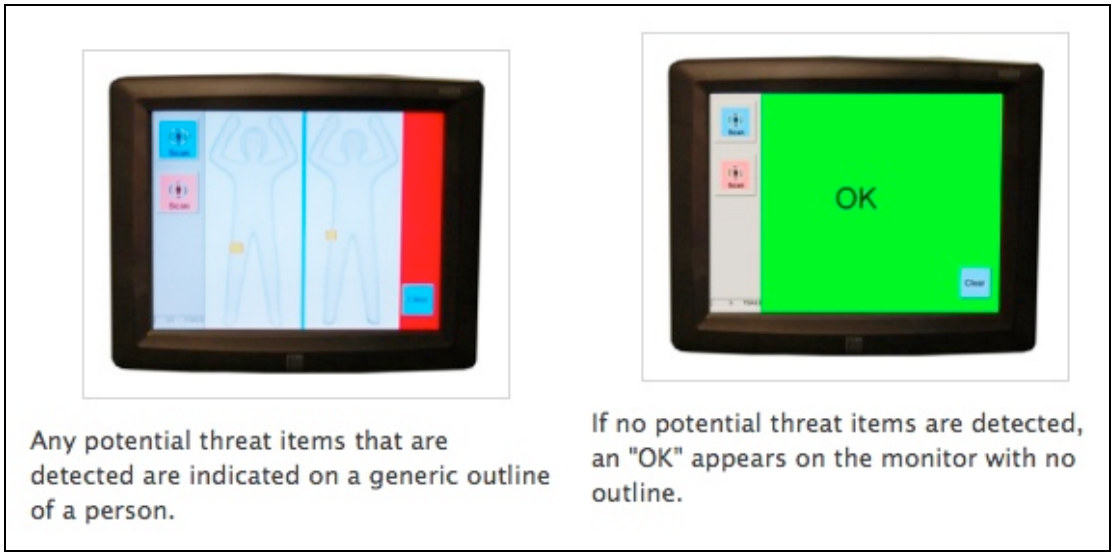

Figure (4): Depiction of an external monitor displaying ATR software

According to the TSA "the use of ATR software will reduce the impact to individual privacy by eliminating the image of each individual's body that is generated by the Millimeter-Wave and X-Ray Technologies (sic!), while still allowing appropriate recognition of anomalies" (ibid., 2011: 5).

Despite being open to several interpretations, an anomaly generally describes something that deviates from what is standard, normal, or expected (Oxford Dictionaries, 2013a). The possibility of using ATR software had already been mentioned by the TSA in 2010 but due to poor detection rates the technology had been subjected to further development and refinement (Burns, 2010a). The first tests of ATR software occurred in early 2011 and were directly related to insecurity of passengers with AIT screening as:

> "A small percentage of travelers have had privacy concerns with the AIT machines… TSA has implemented strict measures to protect passenger privacy, which is ensured through the anonymity of the image… The image is on a monitor that is attached to the AIT unit in public view. Because this eliminates privacy concerns, we no longer have to staff an officer in a separate room" (Burns, 2011a).

Hence, in addition to promises of better privacy protection, ATR software also adds operational and cost-reducing benefits by eliminating the need for a remote image operator.

The modification allows the TSA to forego the use of a second TSA officer who was formerly placed in a “resolution room” occupied with interpreting AIT images from the scanners. While ATR software is applied to scanners around the nation, the TSA also explains practices of remaining backscatter-machines:

> “These resolution rooms are still used in locations where backscatter machines are in place. The officer who assists the passenger never sees the image the technology produces and the officer who views the image is remotely located in a secure resolution room and never sees the passenger. The two officers communicate via wireless headset. The resolution room is used only for the viewing of the images and is not a gathering place or break room for other officers as the officer viewing the images has to be focused in order to prevent any dangerous items from entering the airport” (Burns, 2013b).

Consequently, as ATR takes over the action of interpretation from a TSA officer, discussions regarding the software also include “the general problem of machine vision; namely, how can computers be made to do what we humans do so easily and naturally?” (Dudgeon & Lacoss, 1993: 3). While human interpretation generally relies on experiences and impressions of individuals, the technical perspective of ATR software refers

> “to the use of computer processing to detect and recognize target signatures in sensor data. The sensor data are usually an image from a forward-looking infrared (FLIR) camera, a synthetic-aperture radar (SAR), a television camera, or a laser radar, although ATR techniques can be applied to non-imaging sensors as well” (ibid., 1993: 3).

Although ATR was conceived within a military setting to automatically recognize targets and thereby decrease a pilot's workload and allow him or her more freedom to concentrate on the target and weapon use, ATR technology is also gaining popularity in non-military settings. The functionality of ATR technology can be based on several different approaches, ranging from pattern recognition to artificial neural networks and model-based target recognition. AIT scanners on airports use the latter approach, which is defined by two main characteristics: “(1) matching of processed sensor data to predictions based on hypotheses concerning the target type, pose, and range; and (2) matching of processed sensor data on the basis of multiple localized features" (Ibid., 1993: 6-7). As the authors argue, successful recognition depends on matching parts and identifying the interrelationships among various parts. Even though AIT using ATR software creates an image of the passenger, the software already works with predefined perceptions about the look, shape and body of the passenger. “In some sense, every ATR algorithm is model based because every algorithm makes and uses

a priori assumptions about target and clutter characteristics" (ibid, 1993: 7). Applying the concept of ATR to security searches at airports these assumptions turn out to be estimated from a pre-defined model of the human body. The degrees to which these bodies differ from the preconceived model of a normal citizen determines what is regarded as a problematic or unproblematic body. Deliberations on how a body is supposed to look follow a general paradigm: "First form an initial set of hypotheses based on the sensor data (the *indexing* problem), then use the hypotheses to predict features and their relationships, and finally compare the predictions to features extracted from the data" (ibid, 1993: 7). Despite knowledge of the basic functionality of ATR software the TSA keeps knowledge close on speaking about the capabilities of the software. As the criteria for evaluating human bodies remain opaque, the obscuring of individual body pictures is also hardly ever spoken about in detail.

1.4.1. Changes in judgment

In comparison to early installments of AIT the application of ATR results in several changes to the screening process. The most far-reaching alteration deals with a shift in the responsibility and power to judge anomalies on the body. Prior to the introduction of ATR software, the analysis process of AIT screening had been described following:

> "TSA has implemented strict measures to protect passenger privacy, which is ensured through the anonymity of the image. A remotely located officer views the image and does not see the passenger, and the officer assisting the passenger cannot view the image. The image cannot be stored, transmitted or printed, and is deleted immediately once viewed. Additionally, there is a privacy algorithm applied to blur the image" (Burns, 2011a).

AIT screening therefore relied completely on the expertise of a human TSA officer to interpret the pictures generated by the machine (Mironenko, 2011). Hence the ability to autonomously detect had never been a feature of AIT:

> "Viewing of AIT images occasionally requires interpretation of the images. An AIT image with an anomaly that may represent a prohibited item will require physical screening of the traveler before they may proceed into the sterile area" (USDOHS, 2011: 9).

Because the picture created by AIT does not allow a clear identification, the ability of the TSA officer to interpret the anomaly became important. It was his or her responsibility to advise

the 2nd TSA officer to physically screen the traveler and gain further knowledge on the passenger. In this regard, the use of ATR software represents a decisive alteration to AIT screenings that used to be employed at airports. While the former reduces the number of human workers employed at checkpoints, it also alters the interpretation process. Whereas previously an officer judged anomalies and evaluated their dangerousness, ATR independently performs the task of interpretation. ATR software is used to "determine whether it can replace the existing image viewed by the image operator with a generic image on which the location of anomalies are marked" (ibid., 2). As a consequence, the remaining human officer is delegated to check for every anomaly the software renders as a potential threat. This move leads to the exclusion of human intelligence from evaluating the dangerousness of an anomaly in the process of first detection. Still, the TSA officer remains in control over the second detection round, where suspect passengers receive an enhanced pat-down by the TSA officer according to instructions given by ATR software. "The TSO at the AIT will view both the individual and the ATR image. If an anomaly is identified, the physical screening will target the location of the anomaly. If there are multiple anomalies, the individual may receive a full screening" (USDOHS, 2011: 6). However, the TSA indirectly admits that the human officer represents a weak spot in the agency's protection of passenger privacy. In contrast to a fallible human the machine is an infallible detector of threats. That being said, the functioning of ATR software also declares how the surface of a human body is expected to look. There is an inherent understanding of certain body shapes written into the machine's software algorithms that are compared against real bodies of the passengers.

1.4.2. Changes in visibility

Another decisive alteration that ATR software brings to AIT screenings relates to the depiction and visibility that the technology creates. While example images of AIT (see: chapter 1.1) have been shown to the public by the TSA in order to demonstrate the technological capabilities of the scanners, the leaking of images of individual passengers has created negative press for the TSA. However, efforts to minimize privacy concerns have been an area of importance for the agency for quite some time:

> ”Anonymity is preserved by physically separating the image operator from the individual undergoing screening, and by algorithms that either blur or degrade the image of the face of the individual. The officer that is stationed with the individual does not see the AIT image” (ibid., 2011: 6).

When the TSA made continuous promises that the images generated by AIT would not be stored and would be immediately erased, passengers had to rely on the trustworthiness of the agency. To be sure, passengers were not able to look inside the remotely located room where a TSA officer interpreted AIT scans.

In contrast to AIT practices the application of ATR software takes the importance of visibility more seriously. Whereas previously passengers at the screening checkpoint were not able to view any images, they now encounter a generic outline of a human being attached to a monitor of the AIT scanner. Broadly speaking ATR closes down an obscured room where interpretation had been handled before in favor of transparently showing the depiction of a human body to all participants at airport controls: "Because of the greater privacy protections provided by a generic figure, AIT machines with ATR will deploy the image monitor near the AIT machine so that the screening officer can view it, and will not use a remote image operator" (ibid., 2011: 8). The generic outline promises privacy for the passenger by displaying an inoffensive and abstract picture that could represent anyone and thus no one has to take personal. However, it separates the display of a real body from the individual. So while passengers could previously only guess how pictures created by AIT would look like, ATR offers a clear depiction of how the human is seen by the machine.

While alterations in judgment and visibility mentioned above can be regarded independently, they are at the same time also closely entangled with the work of TSA officers. Despite the primary appearance of ATR as a simple layer, the software also takes over the decisive power of control and detection of potential threats. However, this alteration also comes at a price. ATR software obscures the clearance of anomalies and simultaneously restricts the information for the TSA officer who still has the obligation to verify indicated anomalies. As a consequence the only information available to the TSA officer is whether a potential threat remains or not, in addition to an indication of where the threat is located. As the software gives no feedback other than threat/no threat, clearance through the officer can also become an embarrassing aspect of airport security for certain audiences. For example, medical conditions (e.g. bodily scars, ileostomy etc.) and other private knowledge about the state of the human body then have to be shared with TSA officers. Hence ATR "completely removes the need for a remote operator exclusively devoted to the decoding of the images, and de facto reduces operators' scope for interpretation" (Bellanova & Fuster, 2013: 193). Thus passengers can only hope that their body surfaces are not conceived as being "anomalous" and that ATR software goes easy on them. However, when no "OK" appears on the attached

screen of the AIT scanner, the machine indicates that something must be wrong with the person under supervision.

1.5. Research questions

As was shown in the previous chapter, the modifications that accompany the ATR software update on AIT scanners have great consequences for the screening process. While some of the alterations are clearly recognizable, others appear in a more subtle form, while still others may pass completely unnoticed. However, the widespread introduction of ATR software affects like no other alteration the perception of how AIT scanners handle security and privacy at airports. Such technological alternations also contribute to awareness of the TSA, which is eager to restore confidence as a caring and forward-thinking agency. As a consequence the main research question is as follows:

How does a surveillance technology such as AIT with ATR affect and transform perceptions of privacy and security?

1.5.1. On anomalies and detection through ATR software

Detection capabilities of ATR

The introduction of AIT has strongly been linked to affirmations of providing better security via effective passenger screening and threat detection at airports. While the incident on Northwest Airlines Flight 253 provided the opportunity to install AIT scanners without many public or political objections, the smuggling of plastic explosives on board also allowed AIT supporters to argue that this technology uniquely could respond and reach to this new potential threat. With the introduction of ATR software the determination of a potential threat is shifted from a TSA officer in a separated room to the AIT scanner running ATR software. This shift in the detection process is representative of a strong technological dedication that is central to TSA's philosophy. In a statement, TSA Administrator John Pistole underlined the importance of technology for the agency: "Our top priority is the safety of the traveling public, and TSA constantly strives to explore and implement new technologies that enhance security and strengthen privacy protections for the traveling public" (TSA Press, 2011). Attempts to install ATR software rely on strongly promoting the indispensability of the mechanical eye. Discourses on the capabilities of autonomous software in that sense also create perpetual fear using the "rhetoric of insecurity" (Campbell, 1998) that represents security measures as capable of dealing with threats. Nevertheless, opponents also discursively express their opinion on the (in)capabilities of the software, which leads to the question: **RQ 1: How do stakeholders portray the detection ability of ATR software?**

ATR and the materiality of an anomaly

The ability of ATR software to autonomously detect anomalies is regarded as one of the central features of AIT scanners. Yet guidelines for what exactly is or can be conceived of as an anomaly vary significantly, though at the very least indicate a deviation from what is regarded as corresponding to the normal (Oxford Dictionaries, 2013a). Hence, while the meaning of anomaly in this context remains hard to fully grasp, the body with its hiding places remains in the center of vague allegations of serious threats to aviation security. As individual passenger bodies are accused of carrying anomalies, there is a tendency to redirect the notion of an anomaly toward a more concrete and easier to understand materialization of a thing or substance (e.g. explosives, weapons, powders, liquids). To make ATR software's detection process comprehensible and also to justify or denounce invasive controls, stakeholders undertake efforts to promote the idea of what an anomaly actually represents. As a consequence the public is served with imaginations of what ATR software is capable (or incapable) of detecting. Thus it is of interest for this research to follow the discursive strings of how these abstract anomalies come to life in the imaginations of different stakeholders. Therefore the second research question runs as follows: **RQ 2: How do stakeholders define the materiality of an anomaly?**

The human body under scrutiny of ATR

Being at the center of AIT controls the human body can also interfere with efforts related to tracing threats at the airport. In contrast to metal detectors, with AIT emphasis is not placed on problematic metal items (such as a knife or a gun) but rather on the shape of non-normative and thus suspect bodies. While defining the body as a site of anomalies appears problematic in itself (chapter 2.3), ATR transforms the body into a potential source of threats. The software in that sense conceives the body a priori as a host of potential threats. As everyone's body has to be checked, the inevitably assumed occurrence of a threat hangs over passengers like the sword of Damocles. Still, it has to be questioned after whether detected anomalies correspond to real threats as the TSA suggests or whether they instead represent imaginations of non-normative bodies that fail to pass the surveying gaze of ATR software. Therefore, the third research question runs as follows: **RQ 3: How does the human body interfere with the detection of anomalies?**

1.5.2. On human-machine interaction and the perception of privacy

Effects of ATR on passenger privacy

With the leaking of several thousand passenger photographs from AIT scans (Johnson, 2010) trust in the TSA and its staff reached a low point. The introduction of ATR software had several reasons, with restoring confidence in the agency and emphasizing its dedication to pursuing the use of technology to provide security as main points. It is important to recall former problematic practices of AIT that are defused by the agency through the use of a "technical fix" (Robins & Webster, 1989) that responds directly to privacy concerns by passengers. While individuals find themselves in the middle of a massive AIT scanner that rigorously examines the human body with fast rotating antennas, ATR software redirects attention to the visual output of the device. Fears of leaked images as well as the detailed display of naked individuals are addressed through ATR and labeled a concern of the past as only a generic outline of the passenger remains. Privacy in that sense is "enhanced" and promotes the image of a caring TSA as well as allowing for a rebuilding of trust in the agency. Additionally the shift towards ATR software is discursively emphasized through other benefits that come as a welcome modification and raise ATR software above alternative screening methods of enhanced pat-downs. Still, with former practices of AIT checkpoint controls in mind, the introduction of ATR software appears in the light of privacy violation involving the naked human body. Whereas the TSA expects its passengers to (virtually) lose all their clothes in front of the nation's gaze, society makes its citizens continuously aware of the importance of being properly dressed in public (Allen, 2011). Paradoxically, ATR software firstly "uncovers" the passengers, only to later attempt to "cover" depiction through the use of a generic outline. Again, it remains important whether stakeholders perceive a modification to an invasive technology to be sufficient enough to calm down concerns. Hence, the fourth research question runs: **RQ 4: How do stakeholders portray the effects of ATR software on passenger privacy?**

ATR and the perception of TSA officers' work

One of the main tasks of TSA officers is to provide for fast and straightforward control processes at airport security checkpoints. Yet the detection of threats remains a task that needs careful attention and does not forgive potentially fatal mistakes. While the introduction of ATR software has been accompanied by strong rhetoric that conceives technology as a key factor to providing security (TSA Press, 2011), the work routine of TSA officers has also

been altered. In dismissing the function of a TSA operator formerly responsible for inspecting AIT scans, ATR software also reduces the ability of the remaining TSA officer to interpret the images (Bellanova & Fuster, 2013). In addition to having reduced information, TSA officers must also face the challenge of ensuring continued passenger movement. Kirschenbaum attests that the necessity of passenger flow-rate generates pressure on the execution of TSA officers work:

> "Bending or ignoring the rules and 'waving passengers through' is one of several adaptive security behaviors reflecting the pressures put on security employees to hasten passenger flow due to economic and peer group pressures and constraints of airport operations" (Kirschenbaum, 2013: 39).

TSA officers in that sense not only represent the human face that guides passengers through the screening process, but they also have to respond to the detection of anomalies by ATR software. With restricted abilities to assess the danger of an anomaly through the use of ATR and a constant pressure to get passengers onto their flights, TSA officers face a difficult task of providing security while simultaneously not offending passengers. Therefore the fifth research question is labeled: **RQ 5: How does the application of ATR software affect the perception of TSA officers' work?**

1.5.3. Generic outline and the display of the human body

The perception of ATR's generic outline

Without a doubt, the most obvious alteration that accompanied the ATR software update is the disappearance of individual bodily pictures. The shift from a visible human body to a generic outline is a central feature of ATR that the TSA seems to never tire of pointing out. It is claimed that passengers are promised some sort of anonymity, as their bodies remain impossible to be identified according to the depiction displayed. However, this kind of disappearance does not correspond to what happens inside the AIT scanner. While scholars have pointed to the "violent tendencies of technologies, which emerge from the processes of abstraction and disintegration, and the effacement of personhood" (Hall, 2009: 449), the visual power that resonates from the open display of a generic image remains seductive. Given our visual culture (Stafford, 1996) it seems of upmost importance both to follow scholarly discourses on the visibility and disappearance of the body and to examine the public perception that stems from the confrontation with the generic outline on ATR software.

Therefore the sixth research question is: **RQ 6: How do stakeholders portray the approach of ATR software to depict the human body with a generic outline?**

2. Theoretical framework

This chapter is primarily concerned with explaining the main theoretical concepts that play a key role in supporting the present discourse analysis. The approach of discourse analysis will itself be further explained in the methods section (see: chapter 4.1, p. 57). Altogether, the theoretical framework section consists of six main areas. First, chapter 2.1 (p. 25) gives an overview of current themes in the area of surveillance and media studies. Second, chapter 2.2 (p. 31) introduces the main surveillance theories that provide the foundation for the deliberations of this thesis. Third, chapter 2.3 (p. 32) deals with the central role of the body as a means for identification and also relates to the history of the body as a signifier. Fourth, Chapter 2.4 (p. 36) engages with the conception of mechanical objectivity as well as with practices of human-machine communication. Fifth, in chapter 2.5 (p. 39) practices of seeing are introduced to point out the great importance that visual alterations of ATR have on the perception of the software in the discursive reality of the stakeholders. Finally, chapter 2.6 (p. 42) discusses to the complex phenomenon of privacy and its relation to the human body that is at the center of the screening process.

2.1. Surveillance, the public, and the study of AIT: The current state of affairs

The study of AIT has mostly centered on health issues, (Orouji et al., 2011) religious concerns, (Thomas et al., 2013) legal issues (Tirosh & Birnhack, 2013; Klitou, 2008), and the role of marginalized bodies (Magnet & Rodgers, 2012) or more explicitly the role of transgendered bodies (Currah & Mulqueen, 2011). Additionally, ethical questions raised by the use of AIT have been discussed (Nagenborg, 2011) as have questions on how to balance security and privacy (Frimpong, 2011). While most of the above studies recognize implications of AIT on individual privacy and also acknowledge the surveillance potential that is inherent to the technology, they remain limited in their approach to rather specialized fields. The goal of this thesis is to depict and compare different public conceptions of ATR (and respectively AIT) in the context of surveillance and security. Here, the media, where opinions from are expressed, contested, and established, represent a key factor in the public's perception. Concern with the media and their representation of surveillance and security is important because they can influence public attitudes in a considerable way.

2.1.1. Surveillance and security in the media

News media are viewed as playing an important role in the shaping of public opinion related to security and surveillance. McCombs (2004) describes this role as the power to:

> "Construct and purvey the symbols, myths and images that embody and represent social problems (e.g. anti-social behaviors, acts of terrorism). Moralizing images of crime and deviance, in turn, signify social disorder or threat through the constitution of certain subject positions (e.g. 'street thugs', 'fundamentalist Muslims')" (Hier et al., 2007: 733).

In addition to shaping imaginations on topics of social interest, the media are also a source for technology-related information (Robinson, 1972). Despite the general perception of the news media as a "government watchdog" in democratic societies, Abe (2004) highlighted the little resistance governments face when unveiling surveillance technology in a study concerned with the introduction of surveillance technology during the 2002 FIFA World Cup. While the media is usually regarded as scrutinizing government actions, in that case it was seen to foster moral panic that resulted in the welcoming of enhanced security measures (Abe, 2004). Many studies have addressed the news media as an arena for the battle of ideas related to a certain technology, such as CCTV surveillance systems (Gill, 2003; McCahill, 2002). Monahan (2010) argues in "Surveillance in the Time of Insecurity" that the media play an important part in the construction of insecurities in the social imaginary. Armstrong and Norris (1999) argue that the media are more likely to portray CCTV as an effective crime-preventing measure that criticizes it. To a certain degree such mainstream media reporting is linked to crises or traumatic events. Schudson argues that US journalists depart from neutral reporting during moments of tragedy, in times of public danger, and also during threats to national security (Schudson, 2002: 41). Barnad-Wills (2011) observes a more nuanced construction of discourses. He describes two evaluative schemas: one that portrays a discourse of appropriate surveillance, drawing upon themes of crime prevention, counterterrorism, and national security, and a second that focuses on discourses of privacy, personal liberty, and Big Brother. In spite of important efforts that investigate the role of the news media and their coverage of surveillance, obvious limitations remain. Research into the political sociology of the news media argues that despite the power of big news corporations the arena of public perception remains a contested space in which several actors wield strong influence (Greenberg, 2005). Schlesinger also extends the conception of influencing opinion leaders to further stakeholders.

> "While it is true that news media are key sites in hegemonic struggles, and that news

discourses regularly articulate the interests of powerful actors, non-official actors, including members of social movement organizations and NGOs (non-governmental organizations), also have the capability to take control of primary definitions" (Schlesinger, 1990 in: Hier et al. 2007: 733).

2.1.2. Habermas and the public sphere

An arena consisting of arguments from diverse stakeholders comes close to what Jürgen Habermas (1997) imagines as a working public sphere. Here, the idea is to overcome restricting features such as power relations in favor of equality and freedom of speech:

> "People's communication should be free and equal without restriction, and people are expected to interact with one another by way not of the steering media (money and power) but of the communicating media (language) ... For such communicative relationships among people to be realized, the accountability and responsibility of each speaker are vital. In other words, the public sphere could be seen as the social space where public matters are articulated so that the rational reasoning of the decision concerning them is guaranteed" (Abe, 2004: 228).

Relying on the imagination of a public sphere is comparable to efforts made by the US government to conduct a commenting period on regulations.gov. While it is certainly questionable whether public comments actually have an effect on airport security legislation, their integration into this discourse analysis enriches the perception of ATR vastly. The inclusion of both the NGO EPIC and the TSA itself also enriches the data.
In reference to Habermas' approach, discourse analysis on AIT allows for a reflection on important stakeholders in society that results in a less partial conception than plain media accounts. In reference to Habermas' conception of the public sphere, current efforts toward AIT discourse analysis in the media will be examined.

2.1.3. Discourse analysis of AIT in the media

The number of studies of qualitative discursive analysis and AIT remains low. Habscheid, Thörle and Wilton (2013) have looked upon discursive practices around AIT in analyzing statements made by members of parliament in Germany, France and the UK. The authors focused attention on a "cultural and linguistic comparison of discursively constructed concepts of security and safety, the criteria and selection procedures for scanning air

passengers and the representation of public checkpoints including the deployed new technologies based on ubiquitous computing" (Habscheid, et. al., 2013: 99). More importantly, Gregoriou and Troullinou (2012) looked into media discourses on AIT by investigating headlines of two UK newspapers (*The Times* and *The Guardian*). The authors combined quantitative media analysis with the support of LexisNexis and supplemented efforts with a qualitative critical discourse analysis. Their main interest was in investigating "how security policies surrounding terrorism are portrayed, reasoned and communicated to the public" (Gregoriou & Troullinou, 2012: 21). They found that the center-right *Times* conceived AIT scanners "as a weapon to be employed in the war against "terrorism", with technology deemed superior to humans, themselves being reduced merely to particles for security staff to handle" (ibid., 2012: 32). On the other side of the spectrum, the center-left *Guardian* has not been "afraid to highlight issues relating to the measure's discriminatory implementation, suggesting here multiple ways in which body scanners can be deemed problematic for everyone" (ibid., 2012: 32). Although the authors deserve credit for conducting early media discourse analyses on AIT, the study already appears to be dated given technological advances. Gregoriou and Troullinou started their data-gathering period in December 2009 and continued data collection for one year. Hence, the analysis misses developments and discourses related to the introduction of ATR software to AIT devices. This is a crucial drawback that hinders the analysis's ability to respond to current practices at airports and the discursive "enhancements" that have been introduced in response to criticism from the public.

2.1.4. Specific theoretical perspective of the thesis

While studies dealing with discourse analysis on ATR could not be found, critical examination of the software has so far exclusively been based at a theoretical level. Scholars have dealt with the creation and circulation of "live data" of the body (Kula, 2011), the aesthetics of mechanical objectivity (Lodato, 2010), and the display and material disappearance of the human body through ATR (Bellanova & Fuster, 2013). While Lodato views mechanical objectivity in relation to an over-enactment of security theater (Schneier, 2009) that tries to appease passengers and also make them aware of manifold threats, this thesis also considers the consequences for TSA officers who encounter ATR technology and whose work routines are undoubtedly linked to practices of enforcing mechanical objectivity. Additionally, mechanical objectivity is also related to questions of detection capabilities. An empirical analysis of discourses will provide insights on how technology is perceived and

which expectations are linked to the use of technology. The approach followed by Bellanova & Fuster (2013) reports on three paradoxes that evolve from the depiction of ATR software. The authors point to a disinterestedness of the software in the body in portraying a generic outline while simultaneously scrutinizing individual bodies. Secondly, they also address the point that the body remains invisible while the machine appears visible throughout. Their third point revolves around critics of AIT practices exemplified by anti-AIT movements that appear in the form of naked citizens demonstrating against the technology. This thesis appreciates efforts made by the authors above but focuses more on the perception that results from the display of a generic outline. It reflects on the display of the software but also takes into account the familiar role of the TSA officer in the screening process. Therefore, the focus lies more on attempts to reinstate trust in ATR security practices at airports. However, despite individual efforts to engage with theoretical perspectives these endeavors remain restricted as they only portray partial areas and therefore isolated aspects of ATR software. While the studies above mention important implications from a theoretical perspective, they do not pose empirical questions on how different stakeholders experience ATR software. This thesis surpasses the editorial bias that is common in the news media and allows in addition to theoretical efforts an empirical examination that sheds light on how technology is encountered in real-life settings.

2.2. Theorizing surveillance

Surveillance studies has taken several different directions over the past decades. Surveillance has long been a part of human history; one recalls, for example, the surveillance practices of the Roman census. However, surveillance has developed into a central aspect of bureaucratic organization in modern society to maintain control over masses of public and private information. As Dandeker wrote ”the age of bureaucracy is also the era of the information society” (Dandeker, 1990: p. 2). These tendencies have been intensified with the introduction of new computer technologies that allow for a more systematic collection and evaluation of data and that forego paper based evaluation methods (Marx, 1988). Modern surveillance theory in that sense understands “surveillance as an outgrowth of capitalist enterprises, bureaucratic organization, the nation-state, a machine-like technologic and the development of new kinds of solidarity, involving less “trust” or at least different kinds of trust” (Lyon 2001: 109ff.).

In recent history, Michel Foucault's “Discipline and Punish” (1975) figures as probably the single most important contribution to surveillance studies. The concept of the panopticon that

relates to the prison architecture by Jeremy Bentham ultimately allowed the surveillance of the many by the few. Many theorists have taken up Foucault's thoughts and refined them, as the basic idea of omniscient visibility is central to many schemes of surveillance today. Practices of unseen observation and self-discipline[4] are encountered on a daily basis -- one recalls the placement of CCTV in public places, for example. In short, the panopticon simply refuses to go away (Lyon, 2006: 4). Foucault's work has been applied not only to the prison setting but also to other areas such as governmentality, biopolitics, or the birth of the clinic. In short, Foucault made important contributions to the debate on surveillance studies, with many of his ideas on control, exclusion, and punishment still present, albeit in different forms (Lyon, 2007: 50).

Another more recent development in surveillance studies is subsumed under the notions of postmodern or post-panoptic surveillance theories. Both terms condense new forms of "vigilance and visibility" concentrating on "technology-based, body-objectifying, everyday, universal kinds of surveillance (Staples, 2000: 11). Postmodern surveillance theories differ most obviously in their approach of highlighting "the disparate arrays of people, technologies and organizations that become connected to make "surveillance assemblages", contrasting the unidirectional panopticon metaphor" (Ball, 2005: 93). Surveillance in that sense has long ago left a state of local restriction as it enables "strong contemporary desires, or urges, to bring surveillance systems together, whether for control, governance, security, profit or entertainment" (Haggerty & Ericson 2000: 609). The term surveillance assemblage can be conceived as a process in which "we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored" (ibid., 2000: 606). Heightened vigilance and the consolidation of information sources create a mentality that is obsessed with managing potential risks. Even though risk management had been undertaken well before 9/11 (Bigo, 2002), the magnitude of that effort has increased considerably. The former preventative approach to risk has been replaced by a preemptive one (Ewald, 2002). This pre-emptive approach transfers surveillance and suspicion towards the general public (Valverde & Mopas, 2004). Closely associated with this state of unease is a constant risk of certain disasters to come. Ulrich Beck's (1986) risk society (*Risikogesellschaft*) strongly influenced scientific and public discourse on security for over two decades. A "risk is not the same as a

[4] "The Panopticon's "potential" for surveillance nurtures self-discipline (causing individuals to "gaze upon themselves") and self-discipline replaces torture as the "paradigmatic" method of social control. Thus where persons themselves and their bodies are turned into "objects", self-surveillance emerges as a practice of control" (Eckermann, 1997: 157).

catastrophe, but the anticipation of the future catastrophe in the present (Beck, 2009: 3). While risks can be calculated, it is impossible to say whether and when they may actually occur. Consequently the "rhetoric of insecurity" (Campbell, 1998), which follows a mantra of "better safe than sorry", allowed the emergence of a "safety state" (Murakami Wood, 2006). Furedi further describes the created atmosphere of an endangered society that "beliefs that humanity is confronted by powerful destructive forces that threaten our everyday existence" (Furedi, 2002: vii). While these destructive forces remain hard to spot, a general perception of a fear of crime is established that depicts "a more widespread problem than crime itself" (Bannister & Fyfe, 2001: 808).

This tightening attitude that conceives the minimization of risks as a main objective is also reflected in security controls at airports. While the use of the scanners remains voluntary today, there is a clear tendency to conceive ATR-based AIT as the de facto screening method of the future that leaves little place for other methods of providing security for travelers. Yet while security appears to be a desirable state, the efforts associated with providing security also come with restrictions that systematically offend certain members of society. ATR-based AIT comprises tendencies that can be subsumed under a specific form of governmentality of unease (Bigo, 2006a). While current security practices work according to a principle that requires citizens to disclose evermore information to governmental organizations, AIT also extracts body-related and thus very private information from the passenger. The gathering of information in this case follows a logic of "body-objectifying surveillance" (Staples, 2000) that as will be demonstrated also introduces a "normative imperative of mobility" (Bigo, 2006a: p. 6) and singles out passengers who are perceived to be of potential risk for airport security. As the body appears at the center of attention of AIT controls, the role of the body as a source of identification will be reflected upon in the next subchapter.

2.3. The body as a source of identification

The body as a source of identification has a long history and the commitment to make use of the human body as an identifier is not a new approach to identification. Generally, biometry (also: biometrics) conceives "the application of statistical analysis to biological data" (Oxford Dictionaries, 2013b). While the technology has come a long way, the basic measurable characteristics of the human body (e.g. color of the eyes and hair, size of various body parts, age, gender etc.) have long been recognized as being a part of one's identity. One of the most prominent representatives of anthropometry was Alphonse Bertillon, who created a

system of identification of criminals that relied on different bodily measurements and markers (Lyon, 2001). Anthropometrical data has been useful in criminology but was also guided by an ethnographic discourse around the construction of criminal tribes, deviant populations and martial races (Sengupta, 2003: 129).[5] The historical background of the body as a means to identification has time and again been stigmatized and closely related to the darker parts of human history. From blond hair to shiny blue eyes and awry noses, dubious claims under the pseudoscientific banner of biological determinism took the biomedical body as a signifier of identity (van der Ploeg, 1999: 42). In the domain of Science, Technology and Society (STS) Londa Schiebinger identified developments in the 18th and 19th century not as belonging to the scientific state of current research but rather to the political realities of that time. The body has also been used as a tool to distinguish between superior and inferior human beings. To reign over the oppressed (such as people of color), sexual and racial bodily traits were used to exclude certain groups from citizenship. At a time in history when the universal rights of man were proclaimed (*1793: Déclaration des droits de l'homme et du citoyen*), the body served as a demarcation tool to back up differences (Schiebinger, 1993). In that sense the body became indisputably inseprable from the person and also the object of judgments involving natural perfections and deviance from it.

Today the human body continues to be used as a source of identification. Surveillance applications such as CCTV, pattern recognition software or even consumer devices, such as fingerprint sensors on laptops make use of (parts of) the body. Within STS van der Ploeg has argued for a philosophical relationship between the body, biometrics, and identity. According to her, the use of biometrics favors the body in matters of identity, identification, and information technology. The body becomes an ultimate source of truth. Biometrics thus represents a "missing link", as the technology "informatizes the body" by transforming it into a "machine readable identifier" (van der Ploeg, 1999). Thus in a world mediated and managed through technology machines can finally understand the human. In the case of ATR, the body is also transformed into a machine readable identifier, although with a decisive difference. Whereas biometrics tries to identify the individual out of a great mass of potential targets, ATR works the other way around: It creates a predefined mold to which passengers must correspond in order to be granted access

[5] The biometric approach has been in use since the 19th and continues to be of high relevance today. Examples of today include the biometric assessment of age of refugees (Farraj, 2011), or the use of "smart" cameras in CCTV (Hornung, et. al. 2010).

2.3.1. Biometrics and ATR: Two of a kind

According to van der Ploeg's definition biometrics involves the collection with a sensoring device of digital representations of physiological (or behavioral) features unique to an individual (e.g. van der Ploeg, 1999: 37). The spectrum of biometrics used is very broad and ranges from fingerprints to iris patterns, physiognomic features and also behavioral characteristics such as voice patterns, typing rhythm or gait. Following Zureik and Hindle, biometrics relies on pattern recognition, which converts images into a binary code by means of algorithms (Zureik & Hindle, 2004: 117). Biometric identification systems can be divided into three basic types. The most common method works as an operational process to identify an individual as the same person who has already been enrolled in the system at an earlier time. Authentication can occur, for example, through matching fingerprints or an iris-scan. A second approach works in the opposite direction. It aims to confirm that the individual has not already been enrolled within the system. This approach is helpful in preventing instances of double dipping. Both approaches rely on comparing biometrical representations, mostly called templates, and checking for compliance of two datasets. The third approach to biometrical identification systems is based on a database of previously enrolled people. This identification ”assumes that the person is already registered in the system, and the biometric system provides a short list of nearest matches to a biometric signature” (Rejman-Greene, 1999 in: van der Ploeg, 1999: 102). The common presentation of biometrics as a control application is one of “unique, positive identifiers” that assure a match with “the digital persona” (Clarke, 1994). Despite this rather strong trust in technology, biometric systems reveal their limited potential on closer inspection.

> “Biometric systems claim only to match the template at enrolment with the signal at authentication within a certain probability. If the window of acceptance is made too narrow, then the inaccuracy of biometric methods results in people becoming increasingly rejected. Conversely, raising the threshold will allow some impostors to be accepted” (Rejman-Greene, 1999 in: van der Ploeg, 1999: 101-102).

A major difference between biometrics and ATR is the focus on persons. Whereas biometrics looks out for the individual, ATR software does not seek to identify unique persons out of a crowd. Rather, ATR orients toward a common assumption of how a body is expected to look. Nevertheless both approaches work by referring to a window of acceptance:

> “Potential targets (detections) are confirmed by comparing target images or feature vectors with a database of target and non-target exemplars. Recognition consists of selecting the best match between the target data and the exemplar database. The

> matching criteria may be ad hoc (e.g., mean-square differences between data and exemplar vectors), or they may be based on statistical assumptions that give the appearance a more rational basis" (Dudgeon & Lacoss, 1993: 6).

In this way, ATR places the human body in line with assumptions based on a database and then moves passengers through to see who fits and who does not. As the scanners have to deal with thousands of passengers every day it makes little sense to create an ever-expanding database. This would be a difficult task in terms because of both the data-storing challenge and the changing appearance of the human body. With the exception of fingerprint structure, the human body can change its shape continuously, for example, through gaining or losing weight over time.

In addition to ATR's focus on certain imaginations of "normative" bodies, the main difference between ATR software and biometrics is exemplified by relying on live information. "The particular form of information that body scanners create is rooted in live information, not stored information" (Kula, 2011: 17). That is, it is not the aim of ATR to check on particular persons stored within databases but rather to match the controlled person against several imaginations of the assumed standard shape of the human body. Instead of comparing and verifying the data characteristics of various individuals stored in a database, ATR software has its very own understanding of what appears to be an unproblematic passenger. As ATR algorithms are modeled based on a priori assumptions of the body, it tries to abstract the abnormal and potential dangerous from the normal (Dudgeon and Lacoss, 1993). However, the initial position for ATR software remains very complex. The software has to deal with several shapes of bodies, including male, female, and child, yet it must be accurate and sharp enough to identify anomalies that don't belong to the human body. One can imagine that a too-large window of body acceptance followed by a terrorist attack would instantly call the functionality of ATR into question. Still, the problem lies not just within adjusting certain parameters of software. The major issue is that in the case of ATR software the individual human body is not the center of attention anymore. Instead, the body one is expected to have is taken as reference. What was once the story of verifying who you are -- such as with the use of ID cards and other forms of biometrics -- has become a story of who you should be and how you should look like. Especially for passengers using external medical devices one could claim this shift as a return to standardized body conceptions:

> "When scanners detect breast prosthesis, implants, amputations, adults' diapers, urinal bags, intimate piercing, or body folds resulting from obesity, the passenger is required to undergo a further search, this time a physical one in the form of a thorough pat-down" (Tirosh & Birnhack, 2013: 6).

It is important to understand that the logic behind ATR software works according to inherent conceptions of a “standardized” human body. The software makes assumptions about how a body is expected to look in order to be able to identify the “other” and - following this logic - dangerous bodies to airport security. While prevalent biometric systems try to identify the individual that has already been inscribed, ATR looks out for the deviant within the masses. As a consequence the chapter of identification of the human body will inform research questions that center around the detection process of ATR software and also shed light on conceptions of what appears to be regarded as a deviant body in society.

2.4. Mechanical objectivity

Whereas the human body is positioned at the center of interest for the TSA and its critics, the detection capabilities of ATR software allow the agency to fulfill its task of providing security at US airports. While humans have provided security over centuries in different settings and empowered by different sovereigns, the abilities of the individual human often appear limited. Our ability to see remains relatively weak, as our senses for smelling and hearing when compared to what nature has equipped many animals with. In addition, two different persons might conceive the same event in a different way. This begs the question of how such differences or variances can be corrected. As in many instances in human history answers were sought in technology and through use of instruments, as it was believed that mechanical devices entail a certain degree of objectivity. This form of objectivity is described as a:

> “Mechanical sense of objectivity, which uses specific instrumentation as guarantor of objectivity (examples include: early 1800’s atlas makers’ use of photographs rather than paintings or drawings, even if the photos were black and white, grainy, and poorly detailed, to guarantee that any personal biases or preferences would be removed from the finished atlas, no subjective artistic cleaning of images)” (James, 2000: 35).

In a way, scientific mechanical instruments become a kind of “super-subject”, more reliable than senses of ordinary humans. In transferring the decision-making of threat detection from a second operator to a machine, images of ”neutral” and ”objective” devices come to mind. For Daston and Galison ”objectivity” has been related to ”epistemic virtues” through certain eras that represent ”norms that are internalized and enforced by appeal to ethical values, as well as to pragmatic efficacy in securing knowledge” (Daston & Galison, 2007, p. 40). Whereas scientists in the pre-modern era tried to capture nature through artistic forms of representations, cameras led to the definition of mechanical objectivity, which means

> ”The insistent drive to repress the willful intervention of the artist-author, and to put in its stead a set of procedures that would, as it were move nature to the page through a strict protocol, if not automatically. This sometimes meant using an actual machine...” (ibid., 2007: 121).

In STS feminist theory, Donna Haraway heavily challenged the belief in neutral photography, stating: “There are no unmediated photographs... only highly specific visual possibilities, each with a wonderfully detailed, active, partial way of organizing worlds” (Haraway, 1988, p. 583). In other words, (scientific) images are amplified by an “objective” gaze that appears neutral and hard to contest; while at the same time it privileges certain views and neglects others. The former is precisely what is implied by taking the human out of the process and replacing it with a machine, as only “the machine stood for authenticity” (Daston & Galison, 2007, p. 129). Mechanical objectivity represented through ATR software in that sense embodies a special form of instrumentation that appears to be free of fatigue, personal preferences, or moods. The knowledge gained from the use of this form of objectivity is rendered viable through the use of a well-calibrated device following a strict script and step-by-step process (James, 2000). In reference to the ATR-based AIT this script and sequence can be viewed (see: chapter 1.2.1, p. 12). There is an inherent repeatability that underlies the concept of mechanical objectivity: it is a device that works (with the exception of malfunctions and maintenance) on an ever-reliable basis, allowing for the planning and design of further steps associated with experiences at airports. Along with arguments on improved privacy for passengers, the move towards mechanical objectivity represented through ATR has also been praised for allowing faster and far less complicated scans. Nevertheless, the TSA is dealing with a highly complicated device that creates complex computations that cannot be interpreted or questioned by the operator. Following this trend, the role of the human operator also shifts from interpreting and verifying anomalies to the simple verification of alarms generated by the machine. The concept of mechanical objectivity supports the discourse analysis as it allows for the enumeration of differences between the work of a machine and that of a human operator that are also tightly connected to perceptions of privacy. In the following section these differences will be the subject of a closer look.

2.4.1. Human-machine interaction

The "user interface", that is, the interaction between humans and machines, has been the site of both successful contact and miscommunication since the advent of the personal computer in the 1970s (Suchman, 2007). The most apparent problems are gleaned from

reflecting upon the term “user”, which by itself restricts a multiplicity of potential users to a single individual (Bannon, 1991). Scholars have argued that programmers, as the creators of user interfaces, can become too immersed in the setting of system development, leading to misunderstandings between how a user interface ought to be conceived:

> “It becomes difficult to imagine the perspective of somebody who does not view a computer system as a logical anatomy, an ontology made of data structures, a set of formal relationships and constraints, and a network of paths for data to move along. Since the programmer is imaginatively inside the system, the very concept of a user interface can be difficult to grasp or take seriously” (Agre, 1995: 73).

Among the attempts to consider the multiple facets of conceiving different users, Woolgar has made an important contribution with his notion of “configuring the user” (Grint & Woolgar 1997). What the authors tries to say by that mean here is that not only are imaginations about potential users worked into the development of a computer system, but the possibilities of interaction as well as the limitations for the user are also composed. In some sense, Woolgar turns around the conventional conception of a user being in control over a system, declaring, “by setting parameters for the users’ actions, the evolving machine attempts to configure the user” (Grint & Woolgar, 1997: 71). Within these developments in this context, Grant and Woolgar vividly demonstrate in a study of a product development trial the various ways in which knowledge is distributed and then gets assembled by different groups. People who were conceived to be on a level with users, such as technical writers responsible for creating a documentation of software use, pointed out problems concerned with the lack of knowledge about users while talking to engineers. Conversely engineers warned about taking users’ opinions too seriously as they were believed to be outsiders who did not understand the technology (Suchman, 2007). As a consequence these perceived deficiencies among users led to suggestions that design should adhere to ideas of “where the market was going”, or “where things were going”, resulting in a very generalized understanding of future computing (Grint & Woolgar, 1997: 78). Hence, Grint and Woolgar argue that the user itself is not conceived as an individual actor, but rather as an “incorporation of the user into the sociomaterial assemblage that comprises a functioning machine” (Suchman, 2007: 190). This assemblage was demonstrated in the so-called Ruth study, in which a subject is asked to connect a printer to a PC using a (as it turned out) plug designed for a previous model. As the authors write: “An adequate interpretation will make the instructions, the printer and Ruth herself all part of the (larger) machine. That is, in the event of a successful outcome, these entities can be said to stand in an adequately configured relation to the machine” (Grint & Woolgar, 1997: 90). Despite being oriented

towards a successful outcome, the expectations of observers within the company also contribute to user configuration and the success of the process. There seems to be a necessity to conceive users as a separate entity as "the user's character, capacity and possible future actions are structured and defined in relation to the machine" (ibid.: 92). To overcome these implications Suchman argues that we should "destabilize the machine as object, to treat the design/ use relation as an uncertain and problematic one, and to open the latter to investigation" (Suchman, 2007: 191). This way of thinking enables to conceive the user as being embodied, adhering to a certain location within a particular, actual and historically constituted site (ibid.: 191).

With respect to the application of ATR I argue that the software has been conceptualized in order to minimize the user's action to a very basic functionality due to privacy concerns. Whereas ATR software puts great emphasis on obscuring the naked pictures of citizens, TSA officers have to deal with a vague outline that tells nothing about the characteristics of the individual human body or about a potential threat. While the theory of Human-machine interaction in this thesis sets out basic conditions for the TSA officer as a user of technology, it is nevertheless important to keep in mind how software constrains the possibilities of the user to relate to the scanning capability of AIT devices. The limited information provided for the TSA officer can result in a problematic verification process that also places the human user in a poor light.

2.5. Practices of seeing

The introduction of ATR software not only changes the way in which detection is enacted on the passenger; it also has strong implications on passengers' visual perceptions of AIT. The "seeing" of the detection process has become a feature of which passengers are now becoming a part. "Seeing is the study of the role of sight in the constitution of social organization and cultural meaning" (Grady, 1996: 8). As a consequence of concessions made by the TSA, passengers are now allowed to view the depiction of their body (although in a form of an abstract generic outline), which undeniably locates them closer to the technology. Along with the use of ATR software passengers get feedback on how the detection is moving along and whether further controls have to be endured. ATR thus alters how AIT can be apprehended visually. While passengers for the first time have the ability to see the results of the detection process, they also become involved in the human-machine interaction. The passenger standing inside the scanner receives feedback that allows him or

her to react to eventual threats and also inform TSA officers about the state of an eventual detection.

As seeing in the case of ATR software is centered on the graphical output of the AIT device on a second screen, practices of visualization remain of great importance. Gary Henry conceives visualizing as a process of constructing designs to represent concepts or to organize information. Henry mentions maps, graphs, tables, charts, and models as examples of visualization (Henry, 1995). Visualization also helps to create meaning as it makes logical ordering possible and helps to clarify expression (Lynch & Woolgar, 1990). ATR software takes the visualization of the passenger out from a locked room where previously only a TSA officer was able to view the images. Then, the software alters images by superimposing a generic outline that looks the same for each passenger. It tells a narrative of the passenger as one of many, whose individual depiction seems of no interest to the TSA. As the depiction is one that appears visually harmless, ATR moves on to depict areas where potential threats might be located. It thus can either tell the TSA officer the story of a harmless passenger or of one perhaps hiding something underneath his or her clothes. As the passenger can catch a view of the generic outline he or she becomes an informed part of the screening process. In being able to actively cooperate with the TSA officer, a common visual basis emerges. This, in turn, leads to a solid ground for cooperation and trust is manifested along with the introduction of ATR software among passengers. On the other hand, abilities of the officer and his or her potential to rely on human expertise have effectively been cut back. TSA officers' work is effectively restricted in seeing decisively less than before the introduction of ATR, where a second officer could describe the graphical output and interpret the pictures that had been made available.

> “The scanner creates, not captures, the image. The digitization of image from the reflection of millimeter wave produces an abstracted image reduced by the medium that cannot be captured by natural senses. It only exists as a function of the medium of real time. It only exists as a function of the technological”. (Kula, 2011: 17).

The image created by ATR software makes it extremely difficult for TSA officers to properly fulfill their professional role, that is, following strict security guidelines without treating passengers as terrorist suspects. However, as privacy implications guided much of the development of how ATR appears to passengers and TSA officers through the depiction of a generic outline, the visual component of the software remains of special interest for this thesis. The display of the software constitutes the relationship between the TSA officer and the passenger and provides a way for passengers to relate to the performance and functioning of the scanners. Insights from visual sociology will inform the present discourse

analysis as they allow putting discursive strategies of stakeholder documents into context and relating them to the visual conceptions that lie behind them.
In the following chapter the concept of Privacy Enhancing Technologies (PET) is introduced by discussing two visible alterations of ATR software: first, displaying the body image through a filter; and second, allowing for equal vision on an external screen. It will be seen how these changes play a decisive role in the perception of ATR by its stakeholders.

2.5.1. Privacy Enhancing Technologies, the filter, and equal vision

The term Privacy Enhancing Technologies (PET) refers to:

> ”Coherent systems of information and communication technologies that strengthen the protection of privacy in information systems by preventing the unnecessary or unlawful collection, use and disclosure of personal data, or by offering tools to enhance an individual’s control over his/her data” (Cavoukian, 2009a: 1).

Whereas manufacturer Rapiscan saw itself confronted with massive problems of transferring PET to Backscatter machines (Burns, 2013a) and consequently all Backscatter devices have been removed from airports (see: chapter 1.1, p. 7), this form of “technological fix” (Robins & Webster, 1989) has been achieved with scanners relying on millimeter wave technology only. A technological fix can be understood as a technological solution to a problem created through the use of technology. Even though ATR software comes with many alterations to the screening process, the depiction of a generic outline remains the most powerful and apparent. The display of a stick figure is also something to which the public can easily refer; it is also easier to describe than the processes of automated detection. Next to discourses on ATR software the visual alterations allow people to literally “see” and conceive changes that come with the update. Two decisive differences that were introduced with the visual representation of ATR software remain. The first takes the form of a filter that suppresses aspects associated with threatening privacy. The TSA refers to the notion of a “filter” on the official blog of the agency as a measure to further protect passenger privacy (Burns, 2013c). A filter in that sense is regarded as a “sieve through which visual stimuli pass before they are perceived” (Friedman, 2011: 192). Kula argues that privacy is strongly connected to the visual: “Because most conceptions of privacy place such a high emphasis on the role of visibility, the TSA tries to accommodate privacy concerns by altering the final visual representation of the image” (Kula, 2011: 13).

> “Ignoring something is more than simply failing to notice it. Indeed, it is quite often the result of some pressure to actively disregard it. Such pressure is usually a product of social norms of attention designed to separate what we conventionally consider “noteworthy” from what we come to disregard as mere background “noise”. (Zerubavel, 2006: 23)

The second main alteration can be explained by referring to the practice of equal vision. Whereas with AIT passengers could only guess if and how many images of them were created, they are now openly presented with the outcome of the image-generating process. Whereas previously passengers were unable to look back upon the gaze of AIT, the software update allows passengers to assure themselves that the images taken do not correspond to a realistic depiction of the individual. While ATR is described as an enhancement to privacy the practice of equal vision shapes much of the discursive understanding that the software communicates to disperse passenger concerns. The depiction of ATR in that sense allows institutionalizing a “mode of control” (Pennings & Woiceshyn, 1987: 85) that projects trust and confidence towards the passenger and mitigates privacy concerns. However the control exerted approaches passengers in an unobtrusive way. This can be related to what Introna and Wood (2004) termed as the “silent nature of information technology” that makes it very hard to criticize the depiction of ATR software, as the creation of bodily pictures moves in the background.

In the following chapter the complex and multi-layered concept of privacy will be opened up in order to both get a general understanding of the term privacy and to relate it to the concept of the body and the seemingly opposing interests of national security.

2.6. The privacy paradox

Privacy is a rather confusing concept to define, in terms not only of its core components of but also of what it means for the individual citizen. Generally speaking, many citizens sense an endangerment of their privacy as public and private organizations invade the state of the individual. In other words privacy is something we the people used to have that now has become something that private and public organizations, through the use of information and communication technology, are taking away from us and are denying us. The widely shared opinion in literature states that privacy is in clear danger and that it is eroding and diminishing. Countless, mostly popular books have warned about the death, destruction, or end of privacy. (Garfinkel, 2001; Whitaker, 2000; Rosen, 2000). Orwellian metaphors of total surveillance (Kaplan, 2001) are as alive as ever and undesired photographs on social

networking services are a reminder of the deep implications of leaving traces on the Internet. Surprisingly, though, while surveys reveal that people are deeply worried about privacy, many do not seem to behave accordingly. For example, citizens routinely give out their personal information and willingly reveal intimate details about their lives on the Internet. Law professor Eric Goldman points out that individuals' "stated privacy concerns diverge from what (they) do" (Goldman, 2002). Canadian scholar Calvin Gotlieb takes the same line in declaring, "most people, when other interests are at stake, do not care enough about privacy to value it" (Gotlieb, 1996: 156). On the other hand, some scholars even see privacy as a potential harmful concept in terms of societal interest. Legal scholar Fred Cate for example conceives privacy as "an antisocial construct … (that) conflicts with other important values within the society, such as society's interest in facilitating free expression, preventing and punishing crime, protecting private property, and conducting government operations efficiently" (Cate, 1997: 29). Privacy is a concept but also a fundamental right that is contested from many sites of society. In the same manner finding a clear definition for the term privacy has engaged scholars around the world for decades.

The problem of defining privacy also stems from the many situations and settings in which it is embedded. Privacy violations can occur in diverse ways, from sensational newspaper articles to the selling of customer information data to technological devices such as AIT that can see through people's clothing, just to name a few examples. Rough differentiations have been made in defining the private in contrast to what can be regarded as the public, with only moderate success. Indeed, it is hard to grasp what exactly is meant under the ever-changing definition of privacy. Lillian BeVier has stated:

> "Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy – and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name" (BeVier, 1995: 458).

Even more so confusing is the contribution by philosopher Judith Jarvis Thomson, who states, "perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is" (Thomson, 1984: 272). Nevertheless, all work is not lost and the undertaking of scholars concerned with privacy has led to a vast literature and many diverting conceptions.

The right to be let alone has clearly become the most important definition of privacy so far. In 1890, Samuel Warren and Louis Brandeis penned their influential article "The Right To Privacy," arguing for the legal recognition of a right to privacy, which they defined as a "right to be let alone" (Warren & Brandeis, 1890). Of major significance, the article not only brought

significant attention to privacy, but also framed the discussion of privacy in the United States throughout the twentieth century (Turkington, 1990). As a consequence of new technological developments at that time the so-called snap camera by Kodak made photography for everyone affordable. In the time of a growing sensationalistic yellow press Warren and Brandeis described new technological developments and their possible harmful effects on privacy, observing that

> "(i)nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops" (Warren & Brandeis, 1890: 193).

In hindsight the conception of privacy as the right to be let alone has become the most influential. Today, almost all US states recognize a number of privacy torts that trace their inspiration back to Warren and Brandeis (Solove et. al., 2006). Nevertheless the conception by Warren and Brandeis remains vague and does not provide much insight on what it means to leave people alone. Some criticism of the article, for example by philosopher Ferdinand Schoeman, even states that the authors "never define what privacy is" (Schoeman, 1984: 14). The paradox here is that privacy sometimes also conflicts with conceptions of security that likewise remain a right for citizens. The airport constitutes a place where more than elsewhere security is sought and the body serves as the location where confirmation of security is undertaken.

2.6.1. Privacy and the (naked) body

Over the centuries, the human body has centuries gained importance as a place of personal retreat and secrecy from society. That has not always been the case. The naked body in ancient Greece was heralded for its aesthetic beauty (as various statues of naked athletes show) but was also understood as a means to erase signs of inequality, a central feature to today's conception of democracy (Burress, 2004). Today, privacy of the body and bodily features has become a substantial right in society. Even more so society expects people to wear clothes most of the time, as we receive "messages that we must cover our bodies, that covering is pivotal and that the ways in which we cover ourselves matter" (Allen, 2011: 47). Tom Gerety, for example, claims that no matter what concept of privacy is applied, it "must take the body as its first and most basic reference for control over personal identity" (Gerety, 1977: 266). Claiming that the body is a private sphere can be used to argue against certain invasive screening practices at the airport. Whether it is the concealment of bodily parts or

secrecy about specific diseases and more generally the physical condition of the self, there are many fields that deserve vigilance and defense of bodily privacy.

Furthermore, in the history of western culture nakedness has been portrayed as being inseparable from sex and sexuality, and has consequently been located in the realm of the obscene and the immoral (Cover, 2003). As a second party enters the space of viewing nakedness becomes inherently sexualized: “Nakedness in contemporary culture is a solo affair, or else it is sexual by virtue of the presence of a gazing second party” (ibid., 2003: 56). Privacy advocates have highlighted the importance of one’s control over his or her body in referring to “the right to do with my body what I wish, and the right to control when and by whom my body is experienced” (Reiman, 1976: 42). This right to control who is allowed to gaze at individual bodies of passengers is effectively denied when undergoing AIT scans. From the moment on people stand inside an AIT device passengers have lost control over their bodily privacy and vulnerabilities they normally disguise under layers of clothing. Even though it remains unclothing oneself in front of strangers is often something uncomfortable, the TSA expects exactly this kind of trust towards the agency. Passengers are asked to forego all their concerns and become merely flesh during the screening process. Whereas governments usually expect their citizens to cover their bodies and permit public nudity only in certain separated areas, the TSA’s enforcement of AIT encourages people to show their (virtual) naked bodies. Additionally the state usually makes citizens believe in equal treatment and emphasizes its disinterestedness in bodily traits, a promise that cannot be kept with the use of AIT, as scanners also discover disabilities usually hidden through clothes (Tirosh & Birnhack, 2013).

Along with other important rulings, US courts have also demonstrated the importance of the privacy of the body, as one court declared: “One’s naked body is a very private part of one’s person and generally known to others only by choice” (Roline & Skalberg, 1998). Concerned with the role of AIT and privacy-related claims there has also been some appreciation of privacy-intruding behavior. While US courts have tended to approve governmental measures concerning security as in the case of identification requirement, the x-raying of carry-on baggage, and the use of magnetometers (e.g. Tirosh & Birnhack, 2013: 17-18), the jurisprudence on AIT screening has been rather reserved. Even though AIT screening has become one of the main security inspection procedures at airports and appears to be staying put for the time being, courts have acknowledged the general implications of AIT on privacy: “Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon his or her personal privacy in a way a magnetometer does not” (EPIC, 2011: 8). Arguably avoiding undergoing a full-body scan at

US airports and opting for a physical pat-down grants some freedom of choice. Nonetheless, invasive touching of body parts and the resulting awkward interpersonal contact does not seem to be a highly attractive alternative. “At that moment, the passenger has little choice (to fly or not to fly, to be scanned or physically touched)” (Tirosh & Birnhack, 2013: 41). Passengers see themselves as being at the mercy of the TSA, without having any knowledge about who sees what and at the same time exposing their bodies to state surveillance (ibid., 2013: 41).

A focus on privacy and the (naked) body allows a critical examination of ATR practices to scrutinize at what price security is sought in a society. While the body remains one of the few safe havens of the individual, the TSA expects passengers to forego all concerns towards search practices of the agency. Insights from this chapter also allow a critical reflection on the humiliating consequences that can arise from offending bodily privacy of individuals.

The next chapter will focus on two seemingly opposing needs of society; guaranteeing individual privacy and guaranteeing national security.

2.6.2. Balancing privacy

Solove conceives privacy as an umbrella term that refers to a wide and disparate group of related things (Solove, 2009). This can be seen as a liberating exercise that frees the researcher from dealing with too many definitions or ones that are either too narrow or too broad. Instead of dealing with rather abstract definitions of privacy, the author argues for focusing on the context in which privacy deliberations or violations are discovered. According to philosopher John Dewey “we never experience nor form judgments about objects and events in isolation but only in connection with a contextual whole” (Dewey, 1938: 72). The context as a starting point for deliberations about privacy is also a key element within the theory of privacy as contextual integrity as formulated by Helen Nissenbaum. Contextual integrity marks a state of perfect balance between norms of appropriateness, and norms of flow of distribution. According to the theory of contextual integrity

> “It is crucial to know the context – who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances” (Nissenbaum, 2004: 119).

A comprehensive and applicable understanding of privacy can only be achieved in relation to a specific context. This venture should not be confused with undermining the concept of privacy itself but rather seen as a wholesome approach that helps to understand various

concerns, be economical, political, or other. As Solove states, “we determine the value of privacy when we seek to reconcile privacy with opposing interests in particular situations” (Solove, 2009: 87). As an example of the conflict between accelerating procedures at the airport and privacy deliberations the Registered Traveller program can be useful. For instance, Sparapani suggests, “Registered Traveler also pose an unacceptable inducement that causes business and other frequent travelers to involuntarily forego their personal privacy for the promise of speed and efficiency in screening.” He argues further, “No one should be forced to choose between privacy and speed” (Sparapani, 2006). In opposition to this view is an understanding of privacy that focuses on society as a whole rather than on the rights of the individual. As law professor William Stuntz argues,

> “Effective, active government – government that innovates, that protects people who need protecting, that acts aggressively when action is needed – is dying. Because it requires swift government responses to security threats, privacy is one of the diseases” (Stuntz, 2006).

As these two examples show, there is a continual tension between, on the one hand, privacy rights of the individual and, on the other, government measures to actively protect citizens. Indeed, it is sometimes argued that these measures require individuals to sacrifice privacy for national security. Many arguments relating to privacy refer to the Fourth Amendment of the Bill of Rights, which states:

> “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (Amendment IV, 1791).

Of particular importance here is the notion of an (un)reasonable search, insofar as it must be first defined what is dangerous, and thus relevant for search and inspection by the government, and what is harmless. With respect to airport screening, the two rival interests are government protection of national security and the protection of individual privacy rights during search procedures. Tirosh & Birnhack argue:

> “…we observe that courts tend to assume that privacy is harmed, without explaining how and why, with the result that the courts almost immediately turn to examine the potentially diffusing measures, namely, a means-end fit examination. This is the case with the judicial treatment of body scanners” (Tirosh & Birnhack, 2013: 20).

Courts in the US in that sense acknowledge the violations of privacy but refuse to really engage in a balancing act between the rights of the individual and the claimed national security needs. While the need to detect all kinds of explosives (including non-metal ones) is described as “acute” (EPIC, 2011: 16), the list of privacy infringements people experience when going through AIT scanning is largely ignored. Instead, government measuers to protect passenger privacy are quoted, such as “the distortion of image, the deletion of the image as soon as the passenger is cleared, and finally, the alternative offered to passengers – opting out of the scanning in favor of a (thorough) pat-down (Tirosh & Birnhack, 2013: 21). As a consequence the allowance of AIT scanners has been established almost as a form of plain necessity:

> “The amount of danger to the public by a person who seeks to blow up an airplane, coupled with the concept of airport boarding gates as analogous to our nation’s borders, has created a situation in the United States where courts may view passenger airport screening searches as virtually per se reasonable” (Kornblatt, 2007: 396).

The subchapter on guaranteeing privacy while also enabling the government to carry out security practices reflects the general paradox that composes much of the debate on privacy and security. It shows processes at work that allow governmental organizations to compromise individual privacy in the name of providing security and how these processes are justified, institutionalized, and normalized. With respect to the analysis of documents this theoretical perspective enables a critical understanding of how stakeholders realize discursive realities with argumentation patterns that refer to notions of security and privacy.

3. Research field

For the purposes of this research, data from various stakeholders concerning the debate over consequences stemming from the use of ATR software will be taken into account. The corpus includes documents from US media (*The New York Times, USA Today*), NGOs (EPIC), government agencies (TSA), and public comments from the website regulations.gov. The data used for analyzing discourses will contain a variety of document types from media reports to newsletters and public online comments**.** The data chosen represent a wide variety of various sources and point of views. In bringing the views of different stakeholders together this discourse analysis tries to give room to diverging positions concerned with the introduction of ATR software to AIT from early 2011 on in the US. It aims to portray different opinions on issues of security, privacy, and efficiency. Most importantly, all of these aspects consider the role of the human body as central to deliberations and concerns over ATR software. The data are regarded as key to drawing and answering relevant questions on the perception of privacy and security and the role that technology plays within these negotiations. What was once the domain of dominant print media has now grown to include new distribution channels (such as TV and Internet) but also different actors, such as NGOs, government agencies, or individuals voicing their opinion.

In her book *The Male Pill* Nelly Oudshoorns embraces a constructivist understanding that regards the media as a laboratory for the societal acceptance of technologies (Oudshoorn, 2003). Following this standpoint I regard the field of media as an important arena in which the acceptance of AIT and also ATR software both socially negotiated and culturally contested.

The US possesses several unique characteristics that make the country interesting for conducting the proposed analysis. The history of terrorism reached a climax with the 9/11 attacks on the World Trade Center. As a consequence the US government has embraced several measures to strengthen airport security. The founding of the TSA, an agency belonging to the US Department of Homeland Security that is responsible for airport security and the prevention of aircraft hijacking, took place only two months after the 9/11 attacks. Quick fixes, so to speak, and immediate reactions have been the priority for the US government so far. In many cases these have been carried out with the introduction of new security technologies that have been set into place with little regard to detailed testing. In most instances the privacy of the individual has suffered and taken a back seat. US citizens often have to deal with disruptions and expanded security controls. It is of special interest for this research to follow the manifold negotiations within the US that make some willing to

sacrifice privacy, while others continue to strongly invoke their right to be left alone. In addition, the density of scanners being put in place makes the US the undisputed leader in promoting AIT technology. In that sense the technology becomes a real experience for many US citizens that go through the scanning process in one of the 160 airports participating today (TSA, 2013c). What is more, as technology moves to improve and embrace new concepts it seems to be just a matter of time until metal detectors, previously standard, will be replaced by AIT on a large scale. In the following chapter the relevant stakeholders for this analysis will be introduced to give the reader a better overview of whose opinions are heard within this discourse analysis.

3.1. Relevant stakeholders

The relevant stakeholders identified for this discourse analysis involve the TSA, EPIC, *The New York Times*, *USA Today*, and Regulations.gov. The TSA takes the central position within this discourse analysis. As the governmental organization responsible for airport security in the US, the agency put AIT into place at airports. In addition, as this technology is regarded by some citizens as threatening their right to privacy, the TSA has undertaken great efforts to discursively convince the public of the correctness of and need for the new security measures introduced. The newsletter system of the TSA is such a channel in which the agency continuously tries to convince and comfort citizens and justify measures taken. Still, as the TSA is a governmental organization there is also great interest from the media to pursue, comment, and also criticize actions taken that are mostly taxpayer funded. In that sense, the TSA not only relies on its own emissions of opinion, it also tries to promote its position in classic media channels such as newspapers. By relying on the written word the print media remains the most accessible and unproblematic media for a discourse analysis.

In contrast to popular media analyses that investigate opinions and trends in newspapers, Internet blogs, or TV shows, the aim of this analysis is to try to provide a more complex picture of what forms discourses on ATR software can take in different spheres of society. The print media is still believed to have a decisive effect on public opinion and continues to have a political weight that should not be underestimated, as it can make use of its political and social power to alter or influence the outcome of a certain debate. In taking two of the most important US newspapers into account, namely *The New York Times,* one of world's most journalistically respected newspapers, and the *USA Today*, the most widely sold newspaper in the US, an interesting blend of US print journalism is represented in this discourse analysis. Two assumptions about this choice were made: Whereas *The New York*

Times is believed to offer a (for a daily newspaper) deeper understanding of the technology and implications of ATR, *USA Today* is expected to relate strongly to privacy issues and also the fears and concerns of individuals. However, as the primacy of print media is long overdue and the time of mass media dominance itself is seen as a thing of the past, at least in the US, it is necessary to expand the field of stakeholders for this analysis.

The choice to introduce EPIC as a relevant stakeholder for this analysis has been made due to several reasons: on the one hand, EPIC is an NGO, meaning an organization that follows its own agenda and seems to be free of governmental interference and outside interests. In addition, EPIC has continuously fought for increased privacy and has taken the TSA more than once to court to scrutinize security measures taken since 9/11. Thus, EPIC represents something like the antagonist of the TSA, an organization that is clearly critical towards TSA measures and that doesn't shy from legal avenues to press its interests. Last but not least EPIC enjoys a good deal of prominence in the US print media. The NGO seems to have become a well-respected authority whose opinion is regarded as being of decisive importance.

The last stakeholder that is used for this analysis was, interestingly, born out of an effort by EPIC to challenge AIT practices of the TSA. In court, EPIC gained a partial success that resulted in the call for a public debate. Thus as a consequence the TSA had to open its screening policy for public commentary on regulations.gov (United States Courts of Appeal [USCOA], 2011). Public commentary is regarded as an extremely important component to this analysis as it gives voice to the average citizen and passenger that has been through AIT screening and also describes personal experiences. It is a contribution from the bottom up and represents an ideal addition to the data field.

Concerning the general data set, documents have been collected from early 2011 on, when ATR software was first tested on AIT scanners at certain US airports. Shortly thereafter the program was expanded as was media interest in the software. Data collection ended in June 2013, a date that marked the end of the public commentary period on regulations.gov. This discourse analysis does not claim to construct a picture of all the discourses available and in that sense also foregoes stakeholders that might be regarded of importance for some. Nevertheless, it seeks to give a decisive picture of the current debate on privacy and security. In introducing the relevant sources for this analysis more deeply I will also refer to the stakeholders that have been excluded from this analysis. In sum, this thesis tries to recognize the complex ongoing articulation among the public, the media, and the state (Kellner, 1990).

3.1.1. TSA – Transportation Security Administration

The TSA is an agency belonging to the U.S. Department of Homeland Security. Its main task is to exercise authority over the security of the traveling public in the United States of America.

> "Following September 11, 2001, the Transportation Security Administration (TSA) was created to strengthen the security of the nation's transportation systems and ensure the freedom of movement for people and commerce. Today, TSA secures the nation's airports and screens all commercial airline passengers and baggage (TSA, 2013d)

As the agency sees aviation threats as continuously evolving and taking on ever more complex forms it strives to "use every tool at … disposal to address those threats and develop methods of combating them. The use of new and innovative technology helps us stay ahead of those intent on harming our nation" (TSA, 2013c). The TSA has introduced several new technologies, among them the Paperless Boarding Pass, Threat Image Projection, Biometrics, Explosive Trace Detection and Imaging Technology (ibid., 2013c).
The agency undertakes preemptive and proactive practices that are justified by the sheer possibility that a certain event might occur, an attitude that corresponds to practices within surveillance society or risk society. The precautionary activity of the agency is built upon the sheer conceivability of horror scenarios and the quest to find adequate answers rooted in technology. "We know there's no silver bullet technology, no cure all, no end-all-be-all; but when used by our highly trained workforce and combined with other layers of security, technology helps close down vulnerabilities" (ibid, 2013c). Hence, next to a commitment towards educated personnel, technology is touted as the main tool of risk assessment and the guarantor of security (Manning, 2002). The organization's aim is to protect the safety of passengers and simultaneously minimize privacy invasions that have in its eyes become necessary to protect the security of US citizens.

> "We are your neighbors, friends and relatives. We are security officers, aviation and surface inspectors, air marshals, intelligence analysts, multi-modal transportation experts and other dedicated professionals who protect the nation's transportation systems so you and your family can travel safely" (TSA, 2013d).

TSA announcements are primarily addressed towards the American traveling public but generally speak to the US community as a whole. It is the task of TSA announcements to convince the public of the necessity and effectiveness of security measures taken. ATR software was introduced by the TSA after strong outrage over "naked scanners" in various media channels.

3.1.2. *The New York Times* and *USA Today*

The news media are regarded as capable of putting certain topics on the agenda of their audiences. In that sense the media "construct" or "signify" reality (Berger & Luckmann, 1969). Still, media theory views audiences as capable of actively interpreting the political and social world represented by the media (Neuman et al., 1992). One of the most recent views on the effects of news media was developed in 1980s and is known as the "negation model" (McQuail, 2005). This underscores the strong attitudinal effects of mass media approaches of framing or priming, but at the same time called for awareness that these effects depend vastly on "predispositions, schema, and other characteristics of the audience that influenced how they processed messages in the mass media" (Scheufele & Tewksbury, 2007: 11). It is argued that the most important effect of mass media is "their ability to confer salience on a topic in the minds of their audience" (Bauer & Bonfadelli, 2002: 151). Journalists therefore select information according to several criteria and frame it for their readers to orient themselves within a subject matter. Thus many people base their knowledge and attitudes only on the basis of mediated information through the media. Mass media have continuously covered technology. The complexity of AIT and ATR software is a great example of how the public becomes informed through media representation. Several studies have found the media to be a significant source of information related to technology (Robinson, 1972) to possibly negative implications thereof (Dunwoody & Peters, 1992; Coleman, 1993). This analysis focuses on two newspapers: *The New York Times* and *USA Today*. Though both have a large share of the market, *The New York Times* is regarded as an elite quality newspaper while the *USA Today* has a more popular feel and perhaps for this reason has a larger national readership (Hoffman et al., 2010). By including two newspapers with differing journalistic styles, a more diverse picture of discourses on ATR software appears. The two newspapers will now be introduced in greater depth.

The New York Times is an American daily print newspaper founded in 1851. Today, it also runs America's most visited news website. As news organization *The New York Times* possesses a sterling reputation and has received more Pulitzer Prizes than any other newspaper. As Page (1996: 17) attested in referring to *The New York Times*, "the newspaper features ideas that have been regarded as having the potential to strongly shape public debates." The NYT comes third in terms of national print circulation, after *USA Today* and *The Wall Street Journal*. "The newspaper is owned by The New York Times Company, in which descendants of Adolph Ochs, principally the Sulzberger family, maintain a dominant role" (Wikipedia, 2013a). In a media bias study from the University of California *The New York Times* was given a score of 73.7 points, with 0 indicating most conservative and 100

indicating most liberal. That ranks *The New York Times* perception of readers as 2nd most liberal of all newspapers regarded, following the Wall Street Journal (Groseclose & Milyo, 2004). In contrast to *USA Today* the *NYT* features many in-depth reports.

USA Today is a national American daily newspaper founded in 1982 and published by the Gannett Company. The overall largest newspaper publisher within the US, it also holds several broadcast media stations (Wikipedia, 2013b). *USA Today* remains the newspaper with the largest circulation in the U.S. The newspaper is known for its easily readable and understandable stories. While the newspaper has been "long identified with short stories, infotainment, bright colors and its weather map, Gannett's national daily is quietly becoming a serious newspaper" (McCartney, 1997). *USA Today* sells for US$ 1.00 but also is often distributed for free. Within the media bias study from the University of California USA Today was given a score of 63.4 points. That score ranks *USA Today* as the most centrist newspaper in the sample taken (Groseclose & Milyo, 2004).

3.1.3. EPIC – Electronic Privacy Information Centre

"EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values" (EPIC, 2013b). EPIC is a registered non-profit and receives the lion's share of its funding from individual and organizational donations, as well as through the sale of its publications. EPIC claims to have "no clients, no customers, and no shareholders. We need your support" (ibid., 2013b). The EPIC's work is strongly related to issues of consumer privacy. The organization responds to a great variety of issues concerning privacy and the use of electronic devices and data. Some of its most recent efforts involve interventions related to The Smart Grid (A nationwide plan to deliver electricity across the US), the privacy of text messaging, the privacy of electronic health records, and data retention by ISPs (Internet Service Provider) (Oram, 2010). EPIC's work is regarded as largely successful in "leveraging major international concerns like human rights and consumer protection to address more arcane technical computing and communication policy issues, such as encryption standards and data collection practices" ('The Public Voice' n.d.). Even more so important is its work on governmental issues. EPIC remains a strong opponent of security measures ordered by the TSA. The organization has continuously made use of the Freedom of Information Act, forcing the TSA to make security- and privacy-related documents public. In that sense EPIC is regarded as a supporter of individual privacy rights.

Following a lawsuit TSA was forced to allow a public commenting period on body scanners (EPIC, 2013a). Opponents have criticized EPIC and its supporters for taking broadly generalized positions on privacy-related issues that some interpreted as following a "old good-cop-bad-cop routine" (Steinberg, 1995). Additionally, scholars attest to the importance of non-governmental organizations, noting that their specialized focus allows them to dig deeper on certain topics than the news media can. In that sense the efforts undertaken by NGOs provide "more concrete possibilities for political participation in the deliberative process itself" (Curtin, 2003: 115).

3.1.4. Regulations.gov

Regulations.gov is a US federal government website that acts as an "Internet portal and document repository" (CeRI, 2013) allowing members of the public to participate in the rulemaking processes of federal government agencies:

> Regulations.gov is a multi-agency website where citizens can view and comment on federal regulations and other agency actions that affect their daily lives. More than 35 federal departments and agencies participate in Regulations.gov, which is designed to encourage public involvement and citizen input (US General Service Administration [USGSA], 2013).

Regulations.gov was created and introduced due to "the E-Government Act of 2002's directive to provided the public with Web-based access to, and participation in, rulemaking" (CeRI, 2013). In that sense, the website seeks to encourage the US public to participate actively in the political process through commenting. The FAQ section describes regulations.gov as a "source for information on the development of Federal regulations and other related documents issued by the US government" (Regulations.gov, 2013a). Due to a legal decision by the United States District Court for the District of Columbia, the TSA was forced to make its screening policy public and open for commentaries. Closely followed by the media, this decision was made following a lawsuit filed by a number of privacy and civil-rights groups, including EPIC, against the Department of Homeland Security in 2010. The lawsuit demanded that the TSA conduct "notice-and-comment rulemaking" on the deployment of AIT devices at US airports (United States Courts of Appeal [USCOA], 2011). The website was opened for commentaries for a 90-day period until June 24th 2013. A review of the comments reveals a generally critical tone toward AIT screening at US airports. Comments on regulations.gov are thus also expressions of popular sentiment (Lang & Engel Lang, 1994) that are believed to potentially shape elite actions. In addition, Pierre Martin

highlights the growing importance of public opinion on policy-making, referring here to Canada's security and defense community:

> "Even if one cannot hope to train and certify thirty million experts in foreign and defense policy in the coming years, the public's preferences should not be dismissed as mere whims and moods. It is incumbent upon the policy makers and the broader security policy community to engage the public in a dialogue and to use the available channels of communication – including, of courses, the media – to explain the linkages between the aims of policy, which are widely shared by all citizens, and the means to achieve these aims, which are often matters of contentious debate" (Martin, 2011 in: Caparini, 2004: 28).

Bringing together all of the above-mentioned stakeholders, it is clear that the actors concerned with the discursive negotiation of AIT hail from diverse sectors of society. Nevertheless this picture is far from complete. Two important sources of information are excluded from the analysis: Congressional Hearing Documents and information from the manufacturers of AIT machines. The reasons for doing so will be explained in the following.

3.1.5. Congressional hearing documents

Congressional hearings are an instrument unique to the US Senate. Hearings usually include oral testimony from witnesses and questioning by members of Congress. In the case of AIT and ATR software, TSA administrator John Pistole has made several statements in front of the Senate. These testimonies reflect the basic view of the TSA, the government agency responsible for airport security. Congressional Hearing Documents featuring John Pistole are listed prominently on the TSA website under the rubric Testimonials and have also found their way into the agency's newsletters. They are included as they contribute strongly to the TSA conception of privacy and security. Other individuals have also testified in front of the Senate but these documents are excluded due to their weak visibility in the media debate. Unlike the statements of TSA administrator John Pistole, which are easily accessible on the TSA website, congressional hearing documents have not figured largely in the media debate. In addition, on comments on regulations.gov there are negligible references to Congressional Hearing Documents. Generally, congressional hearing documents tend to go into great detail, meaning that they provide much information that may, however, be too specific and thus fail to give a clear message of how technology is discursively received through the introduction of ATR. In contrast, statements in the print media, the TSA, EPIC, and

regulations.gov provide more to-the-point information and also rely frequently on reoccurring patterns of discourse.

3.1.6. Manufacturers of AIT

The main reason for not integrating the manufacturers is due to only slight differences in argumentation concerning privacy related themes between the TSA and manufacturers of AIT machines. The TSA embraces a technology that mirrors the manufacturers' intentions to find explosives and identify terrorists. In that sense, manufacturers of AIT deliver the tools for the TSA upon which it builds its argument that technology is the key in answering threats and that the machines are essential to fulfill the task of protecting U.S. citizens and passengers. Similar to congressional hearing documents, manufacturers have barely been referred to in the print media debate. It is claimed for this analysis that the standpoint of the manufacturer of AIT devices and the TSA share a common ground and, hence, the integration of manufacturer documents in the analysis would not provide much further insight. On the websites of the most important suppliers of AIT technology information on the technology itself is sparse. While the ability to detect explosive and non-explosive materials is generously presented by the manufacturers, no words are spent on the ATR software itself and there is no information on how the generic outline was conceived or how the automated targeting through the software works (Microsemi, 2013). In that sense manufacturers simply do not take part in the media debate -- executives of the companies are not mentioned -- and all of media's interest is based on the TSA's action of applying AIT screening with ATR software. It seems that the defense industry in general has little interest in being part of media debates as this is mostly associated with critics from various sides. Rather, it is in the interest of companies such as Rapican Systems or Microsemi to do business in an unobtrusive way and without causing too much fuss.

4. Methods

It is the aim of this thesis to reveal the perceptions of diverse stakeholders on privacy and security that accompany discourses on ATR software. Whereas the first two subchapters explain discourse analysis (see: chapter 4.1, p. 56) and qualitative content analysis (see: chapter 4.2, p. 58), both methods will be brought together later (see: chapter 4.2.1, p. 59). Furthermore this chapter will explain the interval of the data gathering period (see: chapter 4.3, p. 60) as well as general data access (see: chapter 4.4, p. 60) and a detailed explanation of the data collection (see: chapter 4.4.1, p. 61). Additionally, the main tool for the document analysis will be introduced (see: chapter 4.5, p. 63), while the last subchapter deals with reflections on data interpretation (see: chapter 4.6, p. 64).

4.1. Discourse analysis

The introduction of ATR software by the TSA is an open move to refute privacy concerns expressed by NGOs, the media, and public opinion. While ATR affects the screening process, the appearance of the technology also changes as the software is discursively renewed towards the public. As part of a qualitative paradigm Terre Blache and Durrheim define discourse analysis as "… the act of showing how certain discourses are deployed to achieve particular effects in specific contexts" (Terre Blache & Durrheim, 1999: 154). How ATR software is represented by different stakeholders within society is therefore linked to certain beliefs on and perceptions of security and privacy at the airport and how these perceptions interact with the human being who is at the center of these deliberations. The same argument is made for discourses on ATR software that are created, debated, and established among the many institutions that form society. "Discourses are broad patterns of talk – systems of statements – that are taken up in particular speeches and conversations, not the speeches or conversations themselves (ibid., 1999: 156). Yet many of these discourses are contested within the sites they are placed, be it the public news media, governmental areas of dispute or an online forum. As a consequence "a struggle for control over discourses is a sign of an ongoing social conflict" (Fairclough, 2001: 73). Terre Blache and Durrheim (1999) describe several strategies that can aid the researcher in identifying relevant discourses. These include, for example: (1) The identification of recurrent terms, phrases and metaphors, as each discourse has a certain way of speaking, including what is said (the content) and how it is said, (2) Awareness of the constellation of an author and a listener -- an analyst must imagine what kinds of people take part in discourses, as well as

become aware of the use of binary oppositions; (3) Finding the inherent logic within every text, as the aim of an individual discourse is to construct a particular truth. Texts have to be examined not in terms of what they *say* but rather in terms of what they *do.* Thus, there is an inherent meaning that lies within a text and it is the task of the researcher to extract these (sometimes hidden) discourses from the text. Hence authors of certain texts share several objectives that are exercised at the same time. These aims can be vary widely but most likely include the desire to convince the reader that the author is venerable and a good person; advance an ideology; or convince the reader to act in a particular way (ibid., 1999).

In contrast to a quantitative methodological paradigm, the use of qualitative discourse analysis demands even more dedication and involvement by the researcher. As Zeeman (2000) wrote, it remains an impossible quest to stay neutral towards examined texts. As the researcher is a part of a specific cultural, historical, and social environment, the analyst also becomes a part of the examined texts' context. It has to be clear that researchers choose certain texts and take excerpts from these texts to put them in a certain order. In choosing how to analyze a text they also achieve certain effects. A possible way to achieve a good balance between following an argumentative plan and still keeping a certain form of openness to the interpretation process is for an analyst to "try to extract him/herself from living in culture, (but) to reflect on culture" (Terre Blache & Durrheim, 1999: 11).
As mentioned above, discourse analysis has been described as an effective approach for revealing a "relation between language and its social reality, especially when it comes to issues of power and ideology and the analysis of inequality in and through language" (Schreier, 2012: 49). Discourse analysis in that sense behaves more like a method and a critical position and attitude towards the research. This strategy has been described in the following way: "What makes a research method discursive is not the method itself but the use of that method to carry out an interpretative analysis of some form of text with a view to providing an understanding of discourse and its role in constituting social reality" (Phillips & Hardy, 2002: 10). While this thesis predominately analyzes discourses to make assumptions about the perception of security and privacy at US airports, it is also based on a qualitative content analysis to, primarily, create a meaningful base of texts for the interpretation.

4.2. Qualitative content analysis

A rather general definition of what can be understood under the notion of qualitative content analysis runs as follows: "Any qualitative data reduction and sense-making effort that takes a

volume of qualitative material and attempts to identify core consistencies and meanings" (Patton, 2002: 453). This rather abstract and general definition is further refined by regarding qualitative content analysis as a method "for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh & Shannon, 2005: 1278). The identification of recurring themes and patterns, guided by a subjective interpretation, also takes on great importance for the analysis of available stakeholder documents on ATR software. To get a better understanding of qualitative content analysis it is also helpful to distinguish it from its quantitative counterpart. While quantitative content analysis has been used mostly in mass communication as a way to count manifest elements within a text (Weber, 1990), qualitative content analysis "was developed primarily in anthropology, qualitative sociology, and psychology, in order to explore the meanings underlying physical messages" (Zhang & Wildemuth, 2009: 308). In contrast to the deductive approach that is used in quantitative content analysis, where hypotheses are usually generated first-hand and then tested against the data, its qualitative alternative is mainly inductive, drawing assumptions directly from the data in the examination of topics and themes (ibid., 2009). Another example of the difference between the two methods differ is found in their way of approaching sampling techniques. As quantitative content analysis relies heavily on the validity of statistical inference, mainly samples with a random or probabilistic logic are applied, whereas "samples for Qualitative Content Analysis usually consist of purposively selected texts which can inform the research questions being investigated" (ibid., 2009: 309). Constituting probably the most obvious points of differentiation from its quantitative counterpart, qualitative content analysis "pays attention to unique themes that illustrate the range of the meanings of the phenomenon rather than the statistical significance of the occurrence or particular texts or concepts" (ibid., 2009: 309).

For this research, the coverage of AIT machines generated a vast amount of documents that cannot be studied in their totality. Therefore, several demarcations had to be made in order to approach the research field. The notions of privacy and security bear different meanings for different people and stakeholders as well as for different settings and time frames. Furthermore, it makes little sense to approach the deep and versatile concepts of privacy and security solely through a quantitative approach of measuring and counting. However, the computer-assisted ability to quickly search through texts and arrange them according to predefined criteria represents a benefit often associated with quantitative methods that likewise remains valuable for qualitative research. Hence, qualitative content analysis has made use of computer programs to aid the research process. For this research, computer

software was used to assist the researcher in organizing, managing, and referring to data in a more efficient way (ibid., 2009), and to keep track of large data sets. For example, software for searching a certain term over a number of articles allowed for a quick overview of the terms that constantly recurred. These efforts were carried out with the software AntConc, which will be further explained in more detail later.

4.2.1. Combining qualitative content analysis and discourse analysis

While some have criticized discourse analysis for being reductive in making use of partial arguments (Widdowson, 1995) or for what is seen as "interpretive positivism" (Fish, 1981) Schreier argues that the combination of discourse analysis and qualitative content analysis is able to refute most of the criticism. Following this approach "Qualitative Content Analysis and Discourse Analysis can be combined by putting the method of QCA into the service of the critical-interpretative attitude underlying Discourse Analysis" (Schreier, 2012: 49). In doing so more structure and traceability is added to the research. In this thesis discourse analysis examines in detail what is written (and what is not) in stakeholder documents, while qualitative content analysis provides a subordinate function that nevertheless remains of great importance for the research process. Most of all, the data-driven creation of categories that assisted the allocation of research questions has been an important help to the research. Hogan (2006) uses the same approach and combines discourse analysis with qualitative content analysis in an effort to uncover power relations and forms of political control in a study of letters to the editor in newspapers during the year after 9/11. Another way of combining the two approaches is to conduct a critical qualitative content analysis. Here particularly Ritsert (1972) as well as Vorderer and Groeben (1987) have engaged with linguistic phenomena that contribute to ideology and power inequalities. As a point of major difference, categories do not refer to textual content but rather to the form of the content and how it is expressed.

4.3. Data-gathering period

As this research is concerned with the implications of ATR software on the public understanding of privacy and security, the focus within the data-gathering period lies with stakeholder documents that deal with ATR software. While the introduction of AIT in the US dates back to 2007, deployment of AIT devices significantly increased after the thwarted terrorist attack on Northwest Airlines Flight 253 at the end of 2009 (see: chapter 1.1.1, p. 9).

As AIT became commonplace at many American airports its general visibility within the media also increased. As a consequence of rising protest and privacy concerns, the appearance of AIT devices underwent dramatic changes (some of them being also highly visible) with the introduction of ATR software. These undertakings were also discursively accompanied by efforts to restore confidence of passengers in AIT devices and the TSA as the responsible agency for providing security at airports. Many of the textual attempts by the TSA render ATR software as an enhancement to privacy, as well as a general progress in efficiency. As the introduction of ATR software is regarded as a unique key event in the history of deploying AIT devices at US airports, I have decided to start the data-gathering period beginning with the testing of ATR software. As a consequence the document analysis starts with February 1st, 2011, the day the TSA first officially mentioned the planned test use of software to enhance passenger privacy in one of their newsletters. The data-gathering period ends with June 24th 2013, the last day of the public commentary period on regulations.gov website, which has helped frame public opinion on AIT and ATR software. Overall, this timeframe of over two years not only features the introduction of and promises associated with ATR software, but is also concerned with ongoing fears of passengers and their responses to discursive and visible changes introduced to AIT scanners.

4.4. Data access

Access to the general data pool was unproblematic. All the sources taken into account can be found on the Internet. They either stem from easy-to-access websites (as it is the case with EPIC.org, TSA.gov, and regulations.gov) or have been collected via the computer-assisted legal research service LexisNexis. Lexis, the predecessor of LexisNexis, was founded in 1973 in the US and has become known primarily for its pioneering efforts in making legal documents electronically accessible. Lexis was followed shortly by Nexis, a comparable product featuring newspapers and magazines in great size and scope (Miller, 2012). Currently, LexisNexis is owned by Reed Elsevier, the British-Dutch publishing giant (Gargan, 1994) and is known as a "leading global provider of content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets (LexisNexis, 2013). The University of Vienna is currently licensing the LexisNexis service and allows its students and employees to make free use of the otherwise fee-based service (Universitätsbibliothek Wien, 2013). The service features a comprehensive collection of the most relevant newspapers and allows for comfortable searching within great sets of databases using keywords. In addition,

LexisNexis allows for the exporting the results in convenient formats such as plain text (.txt). While collecting the data, emphasis was laid on directly saving all texts on a local basis along with tags for the medium and added date. This was done to forestall one of the few problems concerned with data gathering on the Internet: Dead links or documents that have been moved, which make recovery of certain texts a difficult task. This process of data collection was realized manually. All the files were locally stored on the author's computer.

4.4.1. Data collection in detail

To get a first overview of the debate on AIT devices the collection of data started with a rather broad definition of terms to include as much of the debate revolving around AIT as possible. Using the LexisNexis database *The New York Times* and *USA Today* were scanned for the occurrence of at least one of the following terms: `body scan´, `body imaging´ and `security scanner´. These were identified as the most productive terms and synonyms to be used for AIT in a first collection based on several attempts of trial-and-error; more specific definitions such as `AIT´ or ` Whole-body imaging' were not used very often but nevertheless occur within the US media debate to some degree.

The collection and selection of data from the TSA was carried out using the Press Room section (TSA Press, 2013) of the TSA website, which features various kinds of documents including press releases, speeches, blog posts, tweets and, testimony records, which record TSA statements made to government organizations. As argued in the research field section, testimonies in front of the Senate reflect the TSA's view of its efforts toward protecting privacy and guaranteeing security. Tweets, however, were excluded from the data-gathering process. This is due to very short nature of tweets, which are limited to 140 characters each and provide insufficient explanatory power. On the website of EPIC there is a section called EPIC Alert. EPIC Alert is a newsletter publication that appears bi-weekly and covers issues related to privacy and civil liberties in the information age. Among other things the newsletter contains "detailed articles on privacy developments in the US and around the world", as well as "briefing reports on breaking privacy news" (EPIC, 2013c). For both the TSA and EPIC the collection of relevant articles was guided by the same search terms as for the collection of U.S. media articles.

On their websites both TSA (TSA Press, 2013) and EPIC (EPIC, 2013d) feature a section that is termed "In the news". Whereas EPIC lists a comprehensive overview of press publications that feature statements of EPIC in various print media, the TSA accumulates a constricted overview of articles that cite no publications or links to follow. As the US media

play an important role in the analysis, these sections could have proven to be of general importance for the research. Nevertheless, they will not be included, due to the following reason: Both sections represent a biased selection of articles that provide a broad, but also a restricted and one-sided view of what has been written in the media. Instead, the focus on US media will be concentrated on *The New York Times* and *USA Today* and will feature a comprehensive overview of the newspapers and their attitudes towards privacy, AIT screening, and ATR software. This move will strengthen the independence of media articles reviewed and also push the role of the media as a mediator among various stakeholders.

The situation of data gathering on regulations.gov is easier. A docket folder on the website concerning AIT scanning was open for a 90-day period until June 24th at 11:59 PM ET 2013. Participants were able to declare their name or remain anonymous. The proposed document is called NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Regulations.gov, 2013b). Basically, the whole folder is a great data-gathering pool of comments by US citizens that can be easily accessed and searched through. Regulations.gov features the sole category of "comments" that has to be taken into account. Additionally, the comments already share a focus on passenger screening using AIT. In contrast to US media, TSA, and EPIC no primary selection process had to be conducted. Before we turn our attention to the analysis of the documents, an overview of the all the documents that have been saved for further inspection will be made. Whereas the TSA is featured with nine newsletters that met the criteria of the terms "body scan", "body imaging" or "security scanner", EPIC is represented through 25 documents. The media are featured with 31 articles for *The New York Times* and 43 articles for *USA Today*. With respect to regulations.gov, 83 commentaries were identified as relevant. Congressional hearing documents accounted for two writings that were taken from the TSA website. Altogether the main corpus is made up of 193 documents. The low number of only nine TSA newsletters TSA was largely compensated for by news articles and EPIC newsletters that included a number of quotes from the TSA. The sample represents elements of the discourse on AIT and ATR software in the US. It is suggested that the data material is representative for narrative coherences and therefore builds a solid base for a deeper analysis of discourses around ATR software. Representative status in that sense means not reaching for a preferably high number of documents but rather achieving an authentic and plausible theory. Thus representativeness should become visible rather in "consistency and richness of the theory developed" (Konsistenz und Reichhaltigkeit der zu entwickelnden Theorie) and will be achieved by following the dogma of "theoretical sampling" (Strübing, 2004: 81). Theoretical sampling means not following a mathematical order of choosing objects but

rather pursuing a precise discovery of further data material that helps to foster understanding of the research object. As a consequence, theoretical sampling also allows for expanding concepts and categories that share relevance with the research problems raised (Strauss & Corbin, 1996).

4.5. Document analysis: AntConc

After the collection of texts has been achieved a further reduction of the material has to be made in order to be able to make specific statements. Since I am interested in the impact of ATR software on the conception of privacy and security only articles broaching the issue of ATR software are taken into account. To maintain an overview over the vast amount of separately saved text files the use of a tool for document analysis becomes of great importance. A concordance tool allows one to dig deeper into previously overwhelming matters of text and information. A concordance "gives a list of several words, phrases, or distributed structures along with immediate contexts, from a corpus or other collection of texts assembled for language study" (Lextutor, 2013). For the purpose of the thesis the concordance tool AntConc will be used. The term AntConc is a combination of the word 'ant' and tan abbreviation for the word concordance. "AntConc is a freeware, multiplatform tool for carrying out corpus linguistics research and data-driven learning" (AntConc, 2012: 1) It features seven tools for searching within texts and for gaining a quick overview of important elements within large collections of texts. Once the relevant documents were tagged by publication and date they were saved as plain texts using the .txt format. AntConc then allows all of the documents to be loaded into a single matrix. The concordance tool enables searching for specific terms such as "ATR" within all the documents at once. Consequently, all texts listing ATR in their body now appear and can be accessed individually. The software allows for going back and forth among different search terms and documents at all times and is also capable of saving specific searches as separate files.

The analysis was guided by emphasizing the role of TSA newsletters and statements by TSA representatives within all the documents. As a key criterion of the evaluation, statements by the TSA were taken as a vantage point from which certain subjects of interest and discourses were firstly introduced and identified. Recognized patterns of recurring elements were then used within the concordance tool to find similar statements among all the documents listed. As an example, some of these constantly reappearing elements were 'anomalies', 'threats', 'elimination', and enhancement'. Ultimately, this was a process where

many searches had to be made to find the patterns that appeared as common among several stakeholders.

4.6. Data interpretation

Mayring differentiates among three techniques of data interpretation in the context of qualitative content analysis: “Summary, Explication, Structuring” (Zusammenfassung, Explikation, Strukturierung) (Mayring, 2010). All of the techniques can be part of a qualitative content analysis, though each addresses particular needs. Whereas ‘summary’ refers to a strong reduction of the data to reveal core principles of the data, ‘explication’ uses additional data to make sense of texts and testimonies that appear to be out of context. ‘Structuring’ has been identified as the most central technique to analyzing data in qualitative content analysis and seeks to discover the latent structures that are located within corpuses of texts. Mayring sees some important aspects that are key to a successful structuring of data: The basic dimensions of structuring (Strukturierungsdimensionen) have to be derived from the research question and need to be based on theoretical reasoning. The dimensions of structuring are most likely to be differentiated further and segmented into smaller groupings that will lead to the formation of a system of categories (Kategoriensystem). The formation of categories makes up one of the most important processes in interpreting a certain data set. This process can be subdivided into the following three parts: definition of categories, common example (“Ankerbeispiele”), and rules of coding (Haußer et. al., 1982):

Definition of categories: It must be defined with upmost care to which category certain fragments of text belong. The introduction of ATR software is related to three main categories that are also reflected in the array of research questions. The categories deal with (1) providing security through the detection of threats, (2) the perception of privacy through ATR, and (3) the display of the human body through a generic outline. As these categories remained very broad common examples must be listed.

Common example ("Ankerbeispiele"): Example passages of text that represent a category must be mentioned, so categories become more recognizable. These example passages were generated with emphasis on TSA statements on ATR software. In that sense TSA newsletters were used as a vantage point from which categories took on a more concrete shape. After all, the technology was introduced and presented by the TSA to the public and the media; as a consequence, opinions also always relate and refer back to the discursive efforts taken by the agency to promote ATR software. Common examples were dealing with conceptions and understandings of the notion of an anomaly, efforts to

accelerate the screening process, the reduction of personal costs, and enabling equal vision for passengers of ATR software.

Rules of coding: Whenever it is hard to decide for one or the other category rules have to be defined that allow for the categorization of text passages. While Haußer argues for the distinctive creation of exclusive categories, this thesis dealt with several overlaps when assigning stakeholder documents. This problem occurred a few times when newsletters of the TSA addressed several topics within one statement, such as the acceleration of the screening process and heightened security for passengers. Whereas some differentiation of categories could be managed by focusing on specially tailored statements of the stakeholders, some text passages were coded according to several categories.

Within the process of analyzing data it is obvious that the categories need refinement. After all, it takes at least one attempt to fully grasp all the statements in the desired analysis. Therefore, the process of forming categories can be regarded as a cycle. After a first test run imprecise categories had to be adjusted and redefined from scratch. Although the process of categorizing and coding can be regarded as a sufficient technique of analyzing data, Mayring notes that further refinements of analyzing tools are available. Mayring also points to integrating aspects from valence or identity analyses (Valenz- oder Identitätsanalysen) that were conducted by Ritsert (1972). The findings of the process of data analysis can then be interpreted according to quantitative indicators such as frequency, contingency, or configuration (Mayring, 2010). This can be helpful for continuously reappearing definitions and phrases that have stronger emphasis and persistence than others. The TSA has in that sense often referred to the identical use of certain speech patterns were also been taken up by other stakeholders during the investigation period.

5. A stakeholder analysis of ATR software

The following chapter represents the heart of the data evaluation. In accordance with the research questions (see: chapter 1.5, p. 20) three main areas were established. They comprise: (1) anomalies and detection through ATR software (see: chapter 5.1, p. 66); (2) human-machine interaction and the perception of privacy (see: chapter 5.2, p. 82); and (3) generic outline and the display of the human body (see: chapter 5.3, p. 95). Starting with an extensive introduction for each of the three chapters, this is also the section in which the stakeholder documents of the TSA, EPIC, *The New York Times*, *USA Today*, and regulations.gov will be introduced and compared. Additionally, each of the three main areas will be completed with an analysis that reflects on theoretical deliberations concerning the main theoretical concepts (see: chapter 2.2, p. 29). Conclusions drawn within this chapter will also influence he final conclusion and the outlook of the thesis (see: chapter 6, p. 103).

5.1. On anomalies and detection through ATR software

Even though ATR software was primarily introduced to AIT scanners as a means of easing privacy concerns the main purpose of the scanners still lies in their ability to detect. After all, every security technology becomes useless if its ability to detect is not provided sufficiently. Rapiscan Systems, one of the world's biggest providers of AIT detection systems, lists detection ability as its products' most important characteristic on its website. "As the world's leading security screening provider, Rapiscan Systems provides state of the art products, solutions and services that meet our customers' most demanding threat detection needs while improving operational efficiency" (Rapiscan Systems, 2013). However, it is not only the producers of AIT systems that describe detection ability as the most important feature of security technology. The TSA does so as well: on its blog, the agency each week highlights successful discoveries of firearms and other potentially harmful objects to aviation security through the use of AIT. The headline "TSA Week in Review: 30 Firearms Discovered at Security Checkpoints This Week (25 Loaded)"[6] includes a generous illustration of images of weapons as evidence that the technology is able to find potentially lethal objects (Burns, 2013d). Thus, detection remains the main category on which the reliable functioning of security technology is based.

The importance of detection goes back to the early 1970s. As a consequence of a series of

[6] The firearms mentioned in the article have been found in carry-on bags and were not attached to the body of passengers. However, this example illustrates the general importance of successful detection for the TSA.

plane hijackings, in 1972 the Federal Aviation Administration (FAA) introduced metal detectors at airports nationwide, and this turn towards new technological solutions has since been repeated (Wu, 2004). In a statement following the failed attack on Northwest Airlines Flight 253, former Dutch interior minister Guusje Ter Horst underscored the indispensible detection ability of AIT: “Normal metal detectors could not have spotted the explosives, and the use of full-body scanners would have helped prevent Umar Farouk Abdulmutallab from taking them on the aircraft, she said” (Tran, 2009). Hence the ability of AIT to detect dangerous objects is regarded as the key factor for improving security technology. The application of ATR software to AIT scanners allows for the autonomous carrying of the detection process. According to its producers and operators, the software is capable of locating potential discoveries of interest. When operating with ATR software, the TSA calls every indication an anomaly. In the understanding of the TSA, when an anomaly is detected further examination of the passenger is required. Because possible detection demands increased attention by TSA security officers, it also heightens the interest of passengers standing in line. As such, the successful detection of an anomaly creates a state of heightened alertness. Whereas common metal detectors create attention through an alarm sound, passengers using AIT are asked to step out of the scanner and will be subjected to a pat-down. Both scenarios create discomfort and leave the passenger with a feeling of being suspicious. This not only concerns the well-being of the individual but also influences the security process as a whole as it affects a large number of travelers. One citizen vented his anger on regulations.gov:

> A rational person might question whether it is worth the money we are spending to identify anomalies if the vast majority of them (indeed, perhaps all of them) are false positives, and we lack the practical ability to follow up on many of them in any event. This is the height of ineffectiveness. (Regulations.gov, 2013: SD 1)

It must be made clear that what qualifies in the eye of the machine as a potentially dangerous detection tells only half of the story. While detection itself comes as a socio-technical complex process that combines computer hard- and software[7], the construction of discourses around detection can be more easily examined. Hence the justification for why ATR software is regarded as being an improvement or risk to airport security is largely based on a level of different discourses that follow an inherent logic. As a consequence the discourses around the detection abilities of ATR software will be studied from the

[7] This thesis focuses on the discursive construction of the detection process. The analyses of ATR as a socio-technical configuration would break the mold of this work. For the basic concept of the process between AIT hardware and ATR software see chapter 1.3, p. 13 and chapter 1.4, p. 15.

examination of stakeholder documents. In doing so, answers for the first research question will be sought.

Subchapter RQ1: How do stakeholders portray the detection ability of ATR software?

The TSA has a clear understanding of the detection capabilities of ATR software. The agency portrays the software as a key technology for answering threats to aviation security:

> This new software, also referred to as Automated Target Recognition (ATR), will auto-detect items that could pose a potential threat using a generic outline of a person for all passengers. (TSA, 2011: SD 2)

In the statement above the agency associates the term 'items' with a threat. What is very important here is that the agency remains very cautious about the danger that originates from autodetected items. The TSA declares that an item adjoined to the body does not necessarily have to be dangerous to aviation security. Thus, in July 2011 the TSA remained conservative about the detection abilities of the software. The ability of the machine to detect is manifested as an automated process; still, the detection itself needs further investigation by a TSA officer to confirm the realness of a threat. Nevertheless, the work of the scanners is focused on the detection of items. About five months later the agency posted another statement on the detection capabilities of the software in one of their newsletters:

> The ability to safely detect non-metallic threats concealed under layers of clothing provides TSA Officers with an invaluable resource. (TSA, 2011: SD 3)

At this point, there have been now several major shifts in how the TSA addresses the detection capabilities of ATR software. The first is concerned with the attribution of a detection that has gone through a transformation from an item and potential threat to the detection of a full threat. The discourse of a threat that begins as an eventuality has turned into a real threat that is omnipresent and leaves the impression of a potential danger striking at any time. In doing so, uncertainties in detection have also been erased from stakeholder documents of the TSA dealing with AIT. The chance that the ATR software is mistaken is now utterly nil. The TSA argues the software cannot fail and steps back from earlier statements of uncertainty.[8] This opinion shift has been completed in less than two months.

[8] The uncertainty of the agency is displayed foremost in statements from early 2011. In a document from February 2011 that introduced ATR software to the public the notion "potential threat items" is mentioned throughout: "The new software will automatically detect potential threat items and indicate their location on a generic outline of a person that will appear on a monitor attached to the AIT unit. As with the current version of AIT, the areas identified as containing potential threats will require additional screening. The generic outline will be identical for all passengers. If no potential threat items are detected, an "OK" will appear on the monitor with no outline." (TSA, 2011: SD 4)

Whereas the agency first remained cautious about he capabilities of ATR software in February 2011 (SD 4), and later reinforced that argumentation in July 2011 (SD 2) the TSA executes a much firmer route from early September 2011 on. The agency remains committed to this terminology up to today:

> "Advanced imaging technology is one of the best layers of security we have to address the threats of today and tomorrow," said TSA Administrator John S. Pistole. "We remain committed to deploying this integral counterterrorism tool in order to ensure the highest level of security for the traveling public." … ATR is designed to enhance security by safely screening passengers for metallic and non-metallic threats—including weapons, explosives and other objects concealed under layers of clothing. (TSA, 2011: SD 5)

The statement above positions AIT as an integral counterterrorism tool. In doing so the technology is presented specifically as a means to catch terrorist threats The technology is also described as being future-proof: the agency not only promises security for today but also remains concerned with possible future threats. This is regarded as a statement that prides itself in being prepared. As a consequence ATR software is rendered as an indispensable tool that the agency can rely on to provide security for the traveling public. Another major shift is concerned with the location of a threat. The TSA explicitly speaks of a concealed position, which implies an intention of the scanned person to hide something from TSA officers. More concretely this adds a feeling of general suspicion to passengers moving through airport security. Additionally, the ability to detect is being described as safe. Here, the use of the term 'safely' also serves as a reminder of its opposite, that is, dangerous circumstances.[9] There is a tendency within the statement to foster a threatening undertone that can only be appropriately answered with the use of ATR software. Another major change has been attributed to the kind of threat about which TSA speaks: a special characteristic of non-metallic objects. This statement underscores the claimed ability of the software to actively find a certain group of materials. This move can have various reasons but it is certain that the emphasis on non-metallic items highlights precisely that which metal detectors cannot provide (SD 3,5). This has been emphasized through the introduction of AIT imaging in the hope of preventing future terrorist attempts such as that by Umar Farouk Abdulmuttalab in the 2009 Christmas Day "underwear bomb" plot. Another tendency within TSA documents could be attested. By September 2011, the agency has departed from

[9] It is argued that the notion of "safely screening passengers" could also refer to health-related issues that have been raised by critics of the scanners. However this remains unlikely as the TSA until today denies any harmful effects of X-Rays used with early versions of AIT (see: chapter 1.3, p. 14).

general definitions of (non-metal) threats to more substantial descriptions of how these threats can be imagined by the reader. The agency adds weapons, explosives, and other objects to the definition of threat detection (SD 5). In giving a name to these threats, more substance is given to them as well. The agency continues this process in the following statement, in which John Pistole, the TSA administrator, no longer refers to non-metallic threats but rather to very small amounts of powders and other substances like explosives:

> “On the next slide is a small packet of cocaine, discovered by our officers in Indianapolis. It is important to note that what this shows is AITs abilities to detect even the smallest concealed items. In this case, the anomaly was contraband but it shows the technology's capabilities at detecting very small amounts of powders and other substances like explosives - that could pose a threat to the aircraft.” (TSA, 2011: SD 6)

This statement can be seen in a line of sequenced announcements that define the kind of detection with ever more precision. Whereas the shift from a potential to a real threat has already been achieved, the materialization of threats has now also been realized in stakeholder documents. Thus, while descriptions of what is conceived as a threat remained rather abstract in early newsletters, more and more concrete descriptions emerge of what is harmful to aviation security: undetermined descriptions of items turn into concrete substances and powders that are in the same sentence associated with drugs, but also with explosives that could bring down an aircraft. A possible imagination of detection is therefore strongly linked to heavy threats to aviation security, many of them related to terrorist activities. Fears of terrorist attacks are evoked again. The statements from the TSA are however heavily contradicted by arguments from EPIC. The NGO also refers to a very concrete form of a threat, citing the failed Christmas Day attack:

> The system's effectiveness has been called into question, however; documents obtained via EPIC's Freedom of Information Act lawsuit against the Agency reveal that the scanners are not designed to detect powdered explosives like PETN, the explosive used in the failed 2009 Christmas Day "underwear bomb" plot. (EPIC, 2011: SD 7)

The statement by EPIC contradicts the proposed ability of the TSA to spot concrete substances and also recalls the failed bombing attack, which had been the trigger for introducing AIT scanners at US airports. In that sense, both agencies are making use of the failed terrorist attack to build their argumentation on the detection capability of ATR software. Distinctions remain in the use of different time spans. Whereas EPIC refers an event in the past (whereby the associated threat remains today) to illustrate detection incapabilities, the TSA already extends ATR’s detection capabilities to the future. Additionally EPIC does not

speak about items, objects, or general threats but rather about substances that were missed by metal scanners and which the TSA promised would be discovered through the use of AIT. As powdered explosives belong to the category of non-metallic threats one is puzzled by the statement of the TSA claiming detection capabilities. EPIC's statement recalls the limited detection capabilities of AIT scanners, which are not related to the materiality of an item but rather only to the contour and shape that is compared to the outline of the human body. As a consequence, EPIC argues, AIT is not capable of determining the materiality of substances and therefore unable to detect explosives. On the other hand, the discursive strategy applied by the TSA refers to the detection of "a small packet" and immediately links this to substances that may endanger an aircraft. In that sense the TSA misrepresents and overstates the detection abilities of AIT. Basically, the agency promotes the idea that AIT machines are able to locate powders and explosives, although in fact they are only capable of distinguishing the obvious from the not obvious. While John Pistole suggests that AIT machines have a high degree of accuracy, it actually appears that the situation if akin to a blind hen trying to find a kernel of corn. The TSA's logic here is criticized by a commentator on regulations.gov in the following way:

> TSA instead routinely utilizes "proof of concept" analysis and seems to determine that if a hypothesis can be proven, the concept moves forward (such as, the need to find non-metallic explosive material, TSA appears to have asked the question "can these devices find it? Yes. Move forward). TSA should instead consider true data analysis and consider that imaging in general does a very poor job of identifying "anomalies" in general. This fact is well known within scientific circles that use imaging. Anonymous (Regulatons.gov, 2013: SD 8)

The commentator claims that the logic of "proof of concept" eventually results in detection but generally prevents a thorough ability to locate dangers on a body. This can be interpreted as a logic that sacrifices an elaborate security strategy for the sheer possibility of detection. With respect to the ability to detect, the commentator also seems to be rather skeptical. Unlike other stakeholders, the anonymous citizen does not speak of threats. Rather, the commentator insists on using the notion of "anomalies" putting the term in quotes as if to indicate peculiarity or irony. In that sense, all the concreteness regarding 'threats' and 'items' present within TSA and EPIC statements has been substituted by an ambiguous definition of "anomalies". As the commentator conceives imaging technology as doing a poor job he/she claims the TSA should instead aim for a better analysis of their imaging technology capabilities.

Coming back to the research question "**How do stakeholders portray the detection ability of ATR software?,** the TSA presents ATR software as being able to detect all kinds of threats, whether stemming from an item or substance, of metal or non-metal origin. Preceding this strong conviction in technology has been a shift of discourses in stakeholder documents of the TSA that started with the ability of ATR to detect potential threats and developed into an affirmation to identify definite threats. While AIT remains capable of detecting anomalies only, the agency establishes a linkage between anomalies and concrete items and substances. The TSA establishes a chain of reasoning that takes the detection of a "small packet" as a confirmation for the finding of non-metallic threats such as substances, powders, and explosives that are wrapped in the enclosing of a package.

EPIC contradicts this view in parts and links to the inability of detecting powdered substances, as it declares ATR software to be incapable of identifying any kind of substance. This statement is supported by the working principle of AIT. The scanners rely on the emission and reflection of waves (see: chapter 1.3, p. 13) that can create a picture of the surface of the human body but remain incapable of detecting the materiality of a substance. In the same manner a commentator on regulations.gov highlights the general inability of imaging technology to identify 'anomalies' as it remains an open question of what ATR softwares considers to be an anomaly.

As this first introduction to the discourses on detection has shown, there is considerable variation in opinion on the matters at hand. Whereas detection itself remains the main theme of this first part of the analysis there are two subtopics that will be analyzed further: anomaly and the role of the human body in detection. Among stakeholder documents the notion of an anomaly has already been present (SD 6,8) to some extent. Despite the TSA's strict concept of detection that is followed by definitions of threats, which are extensively explained, the term 'anomaly' remains a broad and vague concept.

Subchapter RQ 2: How do stakeholders define the materiality of an anomaly?

One might wonder what falls within the boundaries of an anomaly. Additionally, the notion of an anomaly remains essential for successful detection through ATR software. If we recall the opinion of the commentator at the beginning of the chapter (SD 1) the identification of anomalies leads far too often to nothing or only to the triggering of false positives. A false positive describes the detection of an anomaly that turns out not to be one. Reading the statement, this begs the question of how the TSA and other stakeholders imagine an anomaly within stakeholder documents. In doing so perceptions about what an anomaly represents and means for the reader become apparent. This approach can also be

confronted with statements and experiences from other stakeholders to see whether ATR software corresponds to real life settings at airports. As a consequence, it is in the interest of this research to understand how stakeholders discursively realize the materiality of an anomaly.

In one document released via the Freedom of an Information Act following EPIC's lawsuit, the TSA defines an anomaly as "any undivested objects including explosives, weapons and liquids" (TSA Office of Security Technology [TSAOOST], 2008: 1). The TSA's definition clearly points to a manifestation of an anomaly resembling an object of varying form. Thus an anomaly is understood as something solid, or at least as with the example of liquids as something that is kept in a bag or a comparable type of vessel. This more concrete definition is also approved by a remark from TSA administrator John Pistole made in a speech at George Washington University that was transcribed in one of the agency's newsletters (SD 6). It must be mentioned that the term 'items' is used as a synonym for objects. However the conveyed meaning of an object in a solid form remains valid. In the example the anomaly is equated with a small packet of cocaine or contraband. Pistole continues to emphasize the ability to discover the smallest concealed items and then gives examples of anomalies, naming very small amounts of powders and other substances such as explosives. In doing so the TSA administrator already gives a clear impression of what in his view represents an anomaly. In his statement Pistole also expands the notion of manifested items to include substances. Substances, contrary to items, describe a matter more precisely. If we relate to the example of an explosive object as in the definition given by the TSA earlier (SD 5), a matching description for a substance would be, for example, TNT (Trinitrotoluene). In saying this Pistole implies that the detection mechanism of ATR software goes beyond the mere discovery of an object, that is, that ATR software is capable not only of looking for objects in general but also of finding specific substances. Even though the TSA conceives an anomaly generally as a concrete object or item, the mentioning of liquids and especially powders points, rather, to detection capabilities that also include the identification of substances. The only explanation that would place substances like liquids and powders within definition of an object is when these are transported within a container or repository that would make it possible to carry them on the body without losing them. Nevertheless, by mentioning the capability to detect powders, Pistole automatically enhances the ability of ATR software to recognize very concrete threats such as substances in the form of powders. Consequently. objects no longer remain the only realized detection capability of ATR software through the TSA. This concrete ability to detect substances is opposed by comments on regulations.gov,

who believe that the realization of an anomaly by the TSA and what ATR software detects are two widely disparate things.

> The TSA states that it looks for anomalies through NBS (Naked Body Scanners). TSA is not charged with finding anomalies but rather with finding Weapons, Explosives and Incendiaries. Unfortunately, NBS finds sweat, bra straps, ostomy devices, personal hygiene products, pleats in clothing and often nothing. (Some of that nothing is allegedly found on bare skin.) Susan Richart (Regulations.gov, 2013: SD 9)

The commentator describes many different items that can be indicated by a detected anomaly. Interestingly, Richart also mentions a variety of designated non-items. The commentator names sweat and pleats in clothing, both of which contradict the definition of an item or object by the TSA. The author concludes that ATR often finds nothing, which strongly contradicts TSA's position that the detected objects and substances pose a threat. Following the commentator's argument, the materiality of an anomaly loses concrete form and is described as representing many different forms of materiality and even non-materiality. While once-confidential TSA documents give a rather vague description of what is understood as an anomaly, comments on regulations.gov argue that an anomaly can consist of pretty much anything and does not necessarily relate to a form of materiality or an item or object. By arguing that ATR software often finds nothing, the commentator also denies the software's ability to spot items or even substances on a reliable basis. Whereas John Pistole exaggerates the abilities of ATR software by claiming the capability to detect substances, the commentator denies the ability to find anything concrete, indicating that the software displays various items and non-item and sometimes even nothing at all. Given this apparent multitude of different items and non-items, further questions regarding ATR arise.

As shown above, the realization of what is conceived as an anomaly by the TSA and the identification of an anomaly by ATR software seem to differ widely not only in the TSA's own definition but also when compared to passenger experience. Despite the TSA's claimed focus on items and objects, ATR software detects various items and objects independently from their potential risk to aviation security. Additionally, the software's algorithms identify several anomalies that contradict the definition of an item or object completely.

Coming back to the research question "How do stakeholders realize the materiality of an anomaly?", the TSA discursively constructs an anomaly as a very concrete form of threat. In doing so the agency refers to objects as well as dangerous substances that can harm aviation security. Commentators on regulations.gov, on the other hand, speak of a multitude

of potential findings represented by an anomaly. The realization of an anomaly thus turns into a mundane finding.

Subchapter RQ 3: How does the human body interfere with the detection of anomalies?

The second subtopic centers on the potential effects of ATR detection on the human body. Interference of the body with detection of ATR software becomes apparent as some of the anomalies described above are not only conceived as items on or attached to the body but also appear as part of the individual body, as, for example, the detection of sweat as an anomaly. In that sense the body itself becomes the place of discovery for the appearance of anomalies. This is manifested as a turn that is not mentioned by the TSA but by almost all other stakeholders. This statement from EPIC shows the importance of the surface of the body:

> The Agency asserts that this software can automatically detect "anomalies" on passengers' bodies, and will highlight those areas on the displayed image. If the machine does not detect any threats, it will merely display a green "OK." (EPIC, 2011: SD 10)

One might regard this statement as rather unspectacular, but it tells something important about where the focus for finding anomalies lies. Instead of looking for objects or items, ATR software scans the passengers' body to assess what is regarded as normal and what is not, what is an anomaly and what is regarded as being unproblematic. Only through an examination of the body surface can ATR software indicate areas of interest. While the software algorithm's task is to distinguish the dangerous from the ordinary the decision-making process of ATR software remains a delicate task. As shown earlier the body itself can become the threat as, for example, bodily fluids such as sweat (see: SD 9, p. 74) can make the human appear to be a dangerous individual. EPIC remains very cautious when writing about detection capabilities by ATR software on the body. The NGO puts the word 'anomalies' in between quotation marks, indicating an overall skepticism towards the software's ability to distinguish dangerous from ordinary parts of the body. Alaska state legislator Sharon Cissna gained notoriety after ATR software showed anomalies on her body that eventually turned out to be mastectomy scars:

> Alaska State Representative Sharon Cissna has become a heroine for many women with breast cancer since she spoke out about the "twisted policy" of having the "invasive, probing hands of a stranger" on her, after scanners twice showed the scars

> from her mastectomy and she was ordered to undergo "humiliating" body searches. (NYT, 2011: SD 11)

What the example illustrates is that problems of the detection of anomalies also lead to problems of defining what can be conceived as a “standard body”. The identification of scars from her mastectomy as an anomaly recurred when a second scan was undertaken, which suggests that even very small alterations on the human body can be the trigger for an anomaly detection and consequently be indicated as a potential threat by ATR software. The story of Cissna also found its way into *USA Today*:

> Alaska state Rep. Sharon Cissna in February opted to take a four-day trip by rental car, small plane, taxicab and ferry from Seattle to her home in Juneau after refusing a pat-down. A body scan had shown scars from her breast cancer surgery, which triggered the pat-down. Cissna, a Democrat, says she had been patted down at the airport before and found it invasive, so she did not want to go through it again. (USA Today, 2011: SD 12)

What these examples also show is that the process of scanning passengers tells only half of the story. The detection of an anomaly, no matter how dangerous it really is, leads directly to a more precise investigation of a potential threat, which is carried out through pat-downs by TSA security officers. As seen from the report above, some people find these pat-downs so invasive that they undertake great detours to avoid them. This sort of feeling of "humiliation" is also central in the following excerpt.

> She asserted that the system does not seem smartly tailored to focus on dangerous people rather than "good, law-abiding people." So kids, seniors and those with disabilities, joint replacements and other medical conditions - things they already feel embarrassed about - end up getting harassed. "Not only breast cancer veterans like myself," she said, "but people who've had colostomies, any kind of alteration to their bodies that makes them look not absolutely 100 percent normal. And it is assaultive." (NYT, 2011: SD 13)

The media articles indicate that the TSA applies a narrow approach to a “standard body” that does not allow for alterations. In trying to find very small and also concealed threats the TSA applies detection algorithms along with ATR software that identify any minor deviation from the standard human body that is constructed in their protocol. Some of these alterations can be as harmless as a scar but may cause an embarrassing revelation for the passenger. It is argued in the statement that ATR software discriminates against the already disadvantaged in society. The scanners constantly remind passengers with colostomies, scars from

operations, or ileostomy of their deviance from “standard bodies”. People are over and over again reminded of their restrictions and have to justify themselves in front of TSA officers. Effectively, passengers with a bodily alteration become reduced to this alteration in the eyes of ATR software.

In the above cases the deviation becomes the source of a potential threat. In generalizing the human body as the location of contingent threats ATR software seeks detection among all kinds of bodies:

> "As part of our ongoing effort to get smarter about security, Administrator Pistole has made a policy decision to give security officers more options for resolving screening anomalies with young children," TSA spokesman Nicholas Kimball says. (USA Today, 2011: SD 14)

As some form of concession the TSA has admitted giving more options to carefully resolve screening anomalies. The agency conceives this change in procedure as a continuous learning process. With respect to the human body this is understood as confessing to have insufficient knowledge about common special characteristics and alterations. This policy decision is a step back to a more nuanced approach to security screening that also acknowledges mistakes made by the TSA. While these alterations might be ignored in the case of many groups of passengers, they cause great attention when concerning children, arguably among the most vulnerable groups in society. The software seems to be so rigid that it invades the body of vastly different groups of passengers from people with disabilities, to joint replacements, and people who have a colostomy. In all of these cases ATR software can only distinguish the ‘normal’ from the ‘anomalous’.

As a consequence individual bodies interfere with definitions of a “standard body”. Additionally, alterations of the human body not only interfere with the detection of anomalies but also make the human body a permanent source of suspicion that ATR software is not able to separate from real danger.

The TSA has an ambivalent relationship to the notion of an anomaly. While the agency generally has a strong preference to call a detection through ATR software a threat and puts emphasis on linking the detection to a certain materiality (object/item/substance) (SD 2,3,4,5) the agency foregoes this categorization when it comes to the individual passenger. In the statement in *USA Today* (SD 14) a TSA spokesman explicitly speaks about resolving an anomaly without wasting a word on a potential threat that could be the source of the detection.

This behavior is not a unique phenomenon but reappears also on the TSA website. On a subsite called “Screening for Passengers 75 and Older” the notion of a potential threat isn’t mentioned a single time. Instead, every individual detection is explained as representing an anomaly (TSA Traveller Information, 2013). This behavior leads to the conclusion that the TSA actively talks about ATR software’s ability to detect threats, dangerous objects and substances at a general and abstract level but remains cautious when concerned with the fate of an individual. In that sense the agency favors talking about threats and terrorist dangers that justify the employment of AIT and ATR software than about the possible effects of individual bodily characteristics. On the contrary, other stakeholders represent different views on using the notion of an anomaly. EPIC and commentators on regulations.gov embrace the broadness of the term “anomaly” by putting the notion in between quotation marks (SD 8,10). For these stakeholders, the significance of the term is highly indeterminate, which also points to the outrage felt by many citizens.

In the view of TSA critics, an anomaly as detected by ATR software represents every potential finding, no matter how small and regardless of whether it is dangerous, harmless, or just part of an individual body. (SD 1,11,12,13). An “anomaly” could be anything and following the logic of the TSA anything can become a threat. Citizens express their dissent also in preferring to speak about “anomalies” and generally tending to forego the notion of threats.

Coming back to the research question “How does the human body interfere with the detection of anomalies?”, all stakeholders agree that the body can get in the way of a flawless detection process. The magnitude of interference nevertheless is regarded as being considerably greater when concerned with documents on regulations.gov. It has to be mentioned that the TSA has to deal with several conceptions of “standard” bodies. ATR software needs to be able to relate to different standard conception of the human body that can accordingly be enlarged and also narrowed for different passenger body sizes, such as kids, old people, very thin or obese passengers. Having so many different variables to integrate in the calculation of a “standard” body, ATR software also has to rely on certain expected constants of the human body that tolerate only little deviation. Screening anomalies with children appear to be common and thus also bring the difficulties of ATR software to relate to the bodies of the young to mind.

5.1.1. A discourse of threats

The present chapter presents a more abstract analysis of the **subchapter RQ1: How do stakeholders portray the detection ability of ATR software?**

Coverage concerning anomalies and detection portrays ATR software as a rigid overseer. The agency tries to provide assurance that they are doing everything to protect citizens from becoming victims of hostile aggression in the form of security threats. To achieve this the agency constructs images of ever-present risks and dangers. TSA explicitly speaks about the detection of threats (SD 3,5) and feeds the imagination with exact manifestations of the materiality and consistency of these threats (SD 3,5,6). Furthermost the assurance that is given by the TSA towards the public depicts the strong trust in mechanical objectivity (Daston & Galison, 2007). Technology is portrayed as being able to find every however small threat and avert any danger that is associated with airport security. Trust in technology is enormous as the TSA trusts the devices in taking over the detection process.

The constant mentioning of weapons, threats, and dangerous substances in combination with aviation security fits the notion of a ”rhetoric of insecurity” (Campbell, 1998), a way of speaking that helps to back up unpleasant policy decisions by creating notions of insecurity. A byproduct of this rhetoric is the attempt to foster national identity through the screening process, as is apparent on the “Our People” section of the TSA website: “We are your neighbors, friends and relatives. We are security officers, … who protect the nation’s transportation systems so you and your family can travel safely” (TSA, 2013d). In fostering a sense of community and in reminding citizens to remain vigilant at all time, a feeling of national identity is promoted. Campbell argues that national identity is guaranteed through a “representation of danger” in foreign policy (Campbell, 1998: 3). The bare existence of the “other” in that sense can suffice to produce a feeling of a threat. In doing so the TSA relies strongly on a discourse of threats that has been central to the past decade of American history. TSA statements build upon a trend that was initiated with the 9/11 attacks and has been expanded to include such terms as a whole new “age of terror”, “super-terrorism”, or simply “the new terrorism” (Jackson, 2005). In the same manner as “The War on Terror” stood for a new and persistent dimension of dangers to the sovereignty of the US, TSA time and again feeds imaginations of ever-present terrorist threats. AIT itself is consistently presented as a counterterrorism tool (SD 5). TSA speaks of threats that remain concealed under layers of clothing (SD 3,5,6) and thus hidden from the eyes of security. It is argued that this concealment is also portrayed as cowardice particularly befitting a terrorist trying to sneak into the US. Terrorist behavior remains hidden, tries to deceive, and does not meet the enemy at eye level. While Americans are represented throughout as brave and heroic, the

“other” as depicted through the image of the terrorist hides and runs (Jackson, 2005). As threats remain hidden the vicious intention of a terrorist remains mostly unknown. Further, the textual construction of the agency to safely detect threats (SD 3,5) manifests the “other” as a bearer of omnipresent danger. Making detection a dangerous endeavor establishes a link to the hazardous composition of threats that is exemplified through the use of powders and explosive substances (SD 6), giving rise to images of elusive terrorist threats such from Anthrax and imaginations of homemade bombs.

Another interesting aspect is the TSA's discursive rendering of AIT and ATR software as a security layer to address not only current but also future threats (SD 5). This reasoning corresponds to Ulrich Becks argumentation of existent and non-existent risks. For Beck a risk represents “the anticipation of the future catastrophe in the presence” (Beck, 2009: 3). Reinforcing a discourse of threat the TSA anticipates events that have not yet arrived and thus creates a continuous atmosphere of threat and endangerment. As a consequence the TSA claims relevance for its work and is able to justify security measures taken.

5.1.2. A discourse of materialization

The present chapter presents a more abstract analysis of the **subchapter RQ 2: How do stakeholders define the materiality of an anomaly?**

Detection is inextricably linked to the emergence of an anomaly. Still, the notion of an anomaly remains vague and difficult to contextualize or relate to familiar concepts. This is also because interpretations of what an anomaly can stand or not stand for change through time and experience. In that sense texts and images are “tangible artifacts that a discourse community constructs, recognizes in their own doing, and continues to interpret” (Krippendorff, 2011: 5). As these artifacts are passed from one discourse to another, it is their materiality that is passed on to the receiving discourse community, not their use or what they meant to the source (ibid, 2011: 5). With respect to anomalies this means that stakeholders apply different rhetoric’s of materialization to locate and facilitate the proposed detection capability in accordance with communication with the outside world. Materialization represents the “transformation of ideas, values, stories, myths, and the like, into a physical reality” (DeMarrais et al., 1996: 16). In doing so imaginations of representations emerge and become embedded in knowledge systems of the individual, a nation, or a whole civilization. Effective materialization thus represents a strategic move that makes it possible to “communicate the power of a central authority to a broader population” (ibid.: 16). In doing so the TSA envisions an anomaly as an object only, whereby TSA administrator John Pistole

extends the notion to include powders and other substances (SD 6). Thus the materialization of the notion of an anomaly is not only widened but also deepened. It receives a more concrete orientation that can be classified and stored accordingly to an almost tangible notion of threat. In contrast to the TSA, statements on regulations.gov reconcile a number of very disparate things under the name of an anomaly. In realizing the concept of an anomaly commentators conceive it as an umbrella term that subsumes a variety of objects that do not necessarily pose a danger to airport security. In referring to bodily fluids and pleats in clothing, non-objects are also highlighted as falling under the category of an anomaly. Additionally, in pointing towards the recurring inability of the scanners to find anything at all the TSA realization of an anomaly is contested entirely. Commentators cite here human skin, implying that the surface of the human body seems to have a stronger impact on the detection of anomalies than the TSA claims in its statements (SD 9).

5.2. On human-machine interaction and the perception of privacy

Whereas the previous chapter on anomalies and detection focused on identifying and deterring potential threats, the role of TSA officers and related effects of ATR software now comes into a broader focus. Although related to the processes of detection and verification, emphasis on the work of TSA officers and human-machine interaction also raises important implications and concerns for privacy. As a consequence the work of TSA officers bridges the gap between guaranteeing detection through the verification of a threat and being responsible for providing privacy for passengers during an examination. Hence, this chapter deals foremost with the discursive perception of privacy related to the introduction of ATR software, as well as the influence that ATR software has on the stakeholder's perception of TSA officers' work. In addition, the TSA's difficult financial situation that led to a staff reduction as well a perspective on the 'human factor' are discussed as playing an important role in AIT screening.

5.2.1. TSA's wasteful spending

As mentioned in the previous chapter detection capability was the primary reason for introducing AIT imaging to US airports. Nevertheless, the TSA is concerned not only with successful detection but also how this detection and security can be achieved and at what cost. As a government-funded organization, the TSA lives on a budget and must adhere to tight financial restrictions. Thus, saving money has also becoming increasingly important for the agency as a US House of Representatives report shows: "With an annual budget approaching $8 billion and the tightening of budgets across the board, TSA must eliminate wasteful spending and find ways to do more with less" (Subcommittee on Transportation Security Committee on Homeland Security [SOTSCOHS], 2012: 11). In finding answers to budgetary restrictions and proposed savings, the ATR software update has been identified by the Congressional Research Service as a possible answer financial problems:

> "The anticipated use of ATR in place of human image viewers will eliminate the screener who views and analyzes images in a remotely located viewing room, in most cases. This could reduce system-wide operational staffing for AIT systems by as much as one-third." (CRS, 2012: 10).

Personnel costs are becoming an increasingly important factor for the TSA. The proposed reduction of TSA's workforce by as much as one-third would dramatically ease the agency's financial situation. The intention to save on TSA staff is also a key topic in the U.S. House of Representatives report, in which Representative Mike Rogers writes:

> "TSA's wasteful spending is not limited to technology; it has employed counterintuitive hiring practices during an economic downturn. To date, TSA employs roughly 62,000 people, including over 47,000 screeners, a number that has consistently grown over the last several years. TSA should examine its growing number of employees given the net decrease in the number of people traveling each year in the U.S. … A private sector entity in the face of a shrinking customer base usually must downsize" (SOTSCOHS, 2012: 13).

The reduction of TSA personnel is considered by the report to be a much-needed move and the introduction of ATR software can, according to the CRS (2012: 10) report dramatically decrease the number of TSA officers needed. In the light of financial restrictions it seems sensible to push ATR as standard software and the House report concludes that ATR software is a plausible and worthy solution that should see wider distribution. Still, it would be remiss to only view the introduction of ATR software in financial terms. Whereas financial accountability is an important matter on its own, the most visible dissatisfaction with the TSA stems from the public perception of how AIT has affected US passengers.

5.2.2. Media representations of AIT

It has been almost impossible to overlook the tremendous media uproar regarding AIT, which has been full of sarcasm and sensationalism. Nicknames for AIT abound in the media, ranging from Nude Body Scanners (Hill, 2013) to Naked Full-Body Scanners (Chan, 2013) to the rather dramatic "Porno-Scanners" (Gillmor, 2010). As it has been mentioned in the theory section (see: chapter 2.6.1) being naked remains a very personal decision of the individual (Cover, 2003), that also has to remain a choice of whom to show ones nakedness to (Reiman, 1976). In all these cases the technology has been put in the worst light imaginable in terms of providing privacy for passengers. It is assumed that the introduction of ATR software has in great measure contributed to restoring AIT's poor reputation. After all, the TSA underscores its strong commitment to privacy in the use of AIT.[10] Consequently the

[10]From the section AIT: Privacy: "Strict privacy safeguards are built into the foundation of TSA's use of advanced imaging technology to protect passenger privacy and ensure anonymity, and TSA always

dedication that lies behind the introduction of ATR software also functions as an assurance for passengers that privacy remains an important topic for the TSA and that passenger fears and concerns are being taken seriously. ATR software in that sense is an important chance for the TSA in terms of restoring trust in the agency and its ability to protect passenger privacy. Altogether, the TSA's attempts to better the handling of security and privacy at US airports are guided not so much by relating to the TSA workforce but rather by a strong belief in technology. In accordance with above-mentioned budget restrictions the TSA writes:

> "The Transportation Security Administration (TSA) is undertaking efforts to focus its resources and improve the passenger experience at security checkpoints by applying new intelligence-driven, risk-based screening procedures and enhancing its use of technology" (TSA, 2013f).

Following a risk-based approach, technology is seen as the key element to future improvements in security and also passenger experience. While the engagement of human actors remains an important factor, technology is regarded as a solution for controlling escalating costs. With respect to measures needed to be taken the agency writes: "TSA must accelerate its efforts to optimize screening processes and use of technology to gain system-wide efficiencies" (ibid., 2013f). As the TSA remains under pressure to reduce staff the agency continues to turn to technology for assistance. To further justify this trend, it is argued that the TSA also refers to previous practices regarding efficiency and privacy in which TSA officers were central to the screening process. Therefore the next research question posed is the following:

Subchapter RQ4: How do stakeholders portray the effects of ATR software on passenger privacy?

The TSA argues that ATR software makes it possible to go without the previously employed second screener and improves passenger privacy in the context of reducing screening personal:

> Further, a separate TSA officer will no longer be required to view the image in a remotely located viewing room. In addition to further enhancing privacy protections, this new software will increase the efficiency of the screening process and expand the throughput capability of AIT (TSA, 2011: SD 15).

The TSA argues that despite making a software upgrade, privacy protections by the agency

---

looks for new technology that meets our security standards while enhancing existing privacy protections" (TSA, 2013e).

have already been sufficiently in place. The agency also claims that there once was a need for a second TSA officer, who has been rendered irrelevant through the introduction of ATR software. Even though the agency does not make a direct claim, screening by a human is regarded as being a less-than-perfect solution for ensuring passenger privacy. Thus ATR software provides further measures that shall guarantee individual privacy. The AIT scanner in that sense depicts an efficient and economical technology that protects the privacy of passengers. While AIT and ATR software will not invade privacy, a TSA officer will examine possible anomalies. As a consequence any perceived invasion of privacy becomes detached from the technology and thus turns into a problematic matter for TSA officers alone. Technology in that sense has moved past the need for human assistance in detecting a potential threat and also appears immune to privacy concerns. Human fallibility has also been found among stakeholder documents on regulations.gov. Again here the introduction of ATR software is directly linked to solving problems that occurred when TSA officers were at work:

> 100% ATR is a welcome change and must be preserved. Not only does it address many of the privacy concerns, but it makes AIT more effective by reducing human error. With a human evaluating AIT images, many privacy and security problems may arise (Regulations.gov, 2013: SD 16).

Again, ATR software is regarded as being beneficial for addressing privacy concerns caused by human workforce. Effectively, AIT gains competence through the use of ATR software, as it no longer has to rely on human judgment. ATR software represents an improvement in comparison to human workforce, as the human is regarded as generating situations that can be detrimental to privacy. Again, efficiency is here linked to the foregoing of a TSA officer. Whereas the commentator sees in the application of ATR software a way to address privacy concerns, the general phrasing of the TSA goes one step further. The wording of the TSA's statement on enhancing privacy has already made an appearance in the stakeholder document above (SD 15). The notion becomes a key element of TSA documents as it reappears continuously through newsletters sent by the agency. It is found in no less than five other statements from April 2011 until early 2012. While the phrasing may vary one sentence reappears in the same manner within four newsletters:

> The machines will be deployed with new automated target recognition (ATR) software designed to enhance privacy by eliminating passenger-specific images while improving throughput capabilities and streamlining the checkpoint screening process (TSA 2011, 2012: SD 17,18,19,20)

Despite being similar to other notifications from the TSA, the continuous reappearance fosters this statement in a decisive way. Enhancing privacy has become one of the agency's main assertions. It is argued that ATR software has been developed most of all through placing emphasis on privacy as the core functionality of the software. Generally privacy is conceived as a concept that can be improved by taking certain measures. This time the enhancement of privacy is related to the elimination of passenger-specific images. The second main argument in the statement refers to improvements in throughput and adjustments in the screening process. This is also a reoccurring theme, mentioned in a slightly different manner in a previous TSA statement (SD 15). The mentioning of streamlining the security screening process indicates unification and standardization, while at the same time more passengers will be processed. Coming back to effects of ATR software on passenger privacy *USA Today* also refers to potential improvements:

> The Transportation Security Administration said Wednesday that it has begun installing software to give passengers more privacy when they're screened by some of the full-body scanning machines at airport checkpoints (USA Today, 2011: SD 21).

The newspaper basically echoes TSA's recent announcement. Rather than calling ATR software a further enhancement, *USA Today* writes that passengers will receive more privacy. In other words, the discourse is no longer about an improvement to privacy but rather an enhancement, which carries a stronger impact of adding something that was previously found lacking by many passengers. The article also states that privacy measures were in place and that the use of ATR software increases privacy for passengers. Interestingly enough, *USA Today* writes about the TSA as providing privacy. Privacy is regarded as an external matter that does not belong to the individual but instead is provided as a donation by the TSA. In that sense, passengers receive a kind of gift in the form of a privacy boost. A transfer of privacy as is central to the statement above also reveals the state of passengers being at the mercy of the TSA.

While stakeholders remain critical in their position towards the detection capabilities of anomalies with ATR software and also pointed to continuous mistakes and imperfection of the devices that resulted in privacy violations, the overall perception of privacy in relation to ATR software appears to be more diverse. The statements above also have to be regarded from the position of first encounter towards ATR software. While in the previous chapter (p. ..) stakeholders reported from experiences made with AIT devices (and consequently could also relate to privacy violations) the stakeholder documents from the present chapter relate to a more general perception of privacy that ATR software is suggesting. It is thus not a lived

experience of privacy but rather an imagined and presented conception that has not yet been scrutinized.

The depiction of documents concerned with how stakeholders portray ATR remains generally positive. ATR software is portrayed as being beneficial to passenger privacy. Whereas the TSA relied continuously on a discourse of enhancing privacy (SD 17-20) or further enhancement (SD 15), *USA Today* has incorporated much of TSA speak but focused it on an increase of privacy (SD 21). In addition, commentators see in ATR software the addressing of at least some of the prevailing privacy concerns (SD 16). The role of TSA officers, however, is presented as considerably worse. While TSA officers have in one instance been described as being redundant due to technical improvements (SD 15), some have directly referred to the existence and occurrence of human error (SD 16). Additionally, the benefits of ATR software in terms of enhancing privacy have also been accompanied by improvements concerned with an increased efficiency/streamlining of the screening process (SD 15, 17-20), as well as heightened throughput capability (SD 15, 17-20).

Coming back to the research question "How do stakeholders portray the effects of ATR software on passenger privacy?", the software update is rendered as a strong improvement of privacy compared to the earlier state of AIT airport controls. In referring also to the former state of control where officers examined pictures, a general betterment is perceived. The suggested improvements are accompanied by other beneficial features of ATR software and are in some cases also relied to the foregoing of human workforce. Additionally a limitation of human abilities has also been attested when compared to the performance of ATR software.

Subchapter RQ5: How does the application of ATR software affect the perception of TSA officers' work?

Even though most of the privacy concerns have revolved around the technology of scanners that generate intimate pictures of the human body, the role and work of TSA officers cannot be viewed separately from technology. It is assumed that the everyday performance of the ATR screening process has an effect on how the work of TSA officers at security checkpoints is perceived. Until now a rather critical position has been identified, describing the efforts of TSA officers as being unnecessary (SD 15) but also a source of continuous error (SD 16). Human work is placed at the intersection between passengers and technology. The task of TSA officers is not only to enact exact checks to guarantee security but also to make the screening process convenient for the passengers and as quick as possible. Nevertheless, the application of ATR software alters not only the handling of a scanner but also the work routine of TSA officers. The use of ATR software eliminates the need for a second officer to

view and interpret AIT scans and also establishes a new hierarchy in sequences at airport controls (see: chapter 1.3). According to a commentator on regulations.gov this shift is exemplified through distancing staff from passengers:

> I have been through airport security, which left me feeling secure, was fairly quick, and didn't dehumanize me - in Israel. It is possible to achieve, but adding technology and further distancing staff from passengers is not the way to achieve it. I say this as someone in the IT field: technology isn't always the answer. I have not been physically assaulted by staff who were performing pat-downs after I declined scans, but there have been verbal attempts to intimidate me into getting the scans. Staff who actually patted me down was largely pleasant and respectful. Anonymous. (regulations.gov, 2013: SD 22).

The commentator starts his statement with a desirable example of airport security, which was experienced in Israel. Mentioning the country at the very end of the sentence, set apart by a dash, is conceived as a jab at airport security in the US. The anonymous commentator believes that the same standards at US airports can be achieved but describes the chosen path of adding technology and further distancing staff from passengers as wrong.[11] ATR software is seen as a separator that makes it harder for TSA officers to adapt to certain needs of passengers. The person refers to individual experiences made in the IT field and sees technology as not always being the best answer to apparent problems. While experiences with pat-downs remain acceptable, the commentator sees a problem in how verbal attempts are made to get the person into intimate scans. Following the comment on regulations.gov, cooperation between human workers and AIT is rendered as complicating the screening process. As the example above shows, human workers are also delegated to enforce the use of AIT and ATR software. In relation to the proposed distancing of staff from passengers (SD 22) it is of interest for this analysis to question how documents concerned with the utilization of ATR software further mediate the perception of TSA officers' work. In a statement, TSA's Assistant Administrator for Security Technology Robin Kane reports on the positive effects of ATR for TSA officers:

> "This technology, combined with our many layers of security, gives our officers the best

[11] (Wagner & Bell, 2012): Referring to security practices at Tel Aviv's Ben Gurion airport: "Departing passengers are questioned by highly trained security agents before they reach the check-in counter. These interviews could last as little as one minute or as long as an hour, based on such factors as age, race, religion and destination. Unlike in many western airports, passengers are not required to remove their shoes while passing through physical screening processes. Furthermore, there are no sophisticated x-ray machines; rather, traditional metal detectors are still in operation. Raphael Ron, a former director of security at Ben Gurion for 5 years, calls the passenger-oriented security system more focused on the "human factor", based on the assumption that terrorist attacks are carried out by people who can be found and have been stopped through the use of this simple but effective security methodology."

> ability to detect and deter non-metallic threats," said TSA Assistant Administrator for Security Technology Robin Kane" (TSA, 2011: SD 23).

Robin Kane sees in ATR technology and the many other layers of security a great source of assistance for TSA officers in detecting and deterring non-metallic threats. Technology is conceived as a supporter of human workforce that simplifies and strengthens the ways of detecting potentially dangerous objects. In contrast to the opinion of a TSA official responsible for security technology the experience of a passenger shows a different picture. After a scanner reflected the shadow of an ostomy bag an alarm was raised:

> Fearing that would happen, she had printed out the notification card on the T.S.A. Web site, as she wrote, "so as to discreetly inform the T.S.A. agent of my medical condition. The agent would not even look at the card. ... The screening agent then did a hand search of my groin, breasts, under the waistband of my slacks and around my ostomy bag. ... Does having an ileostomy now make you a terrorist suspect? (NYT, 2011: SD 24).

The passenger refers to a notification card taken from TSA's website in order to report on special (medical) characteristics of the body. It is reported that the agent would not even look at the card, representing a document from the organization for which the officer works. What is interesting in this case is what is not written on the document. Supposing someone would not even look at something indicates that the person relies on different knowledge for making his or her assumptions. Hence the touching of the body did not come from information written on a notification card or verbal information given by the passenger but was solely based on the output of the scanning device. The report portrays the TSA officer as someone clearing potential anomalies but also as a human worker missing the ability to empathize. In that sense the information output of the machine rules over personal information provided by the passenger. This leads to the assumption that the officer is subordinate to the machine. Still, the human officer gets blamed via the news report for following instructions provided by ATR software. In another article in the *NYT* the harsh inspection at the security check point reoccurs:

> John Pistole, the T.S.A. chief and 26-year veteran of the F.B.I., said he called Tom Sawyer, a 61-year-old bladder cancer survivor who had his urostomy bag dislodged, and urine spilled on him, after a rough T.S.A. search in Detroit last November. "I asked him to come in and provide some personal perspective that could be used in training to give greater sensitivity," said Pistole, who flew Sawyer from Lansing, Mich., to Washington. (NYT, 2011: SD 25).

In the same article John Pistole takes a position. After a degrading treatment of a passenger the TSA chief asked Tom Sawyer for a personal perspective. This implies that TSA officers somehow lack sensitivity when clarifying anomalies. In speaking with the passenger personally, John Pistole conveys the impression that the TSA emphasizes with the experiences of individual passengers. Pistole's move here carries a notion of sensitivity to a search experienced as offensive. As the following article will show this unfortunate happening was not a unique scenario but more likely the consequence of a systematic failure in coordination between ATR software and TSA workforce:

> But in July, Mr. Sawyer had another incident with a screener who squeezed his urostomy bag, leading him to conclude that his was not a "one-off" situation, and that there are still holes in the agency's training efforts. "I see a real disconnect between what they say they're doing and what's really happening at the airport," Mr. Sawyer said. (NYT, 2011: SD 26).

The article above reports on the same Mr. Sawyer who experienced an invasive encounter with TSA workforce for a second time about half a year later the first incident occurred. There seems to be repeatability in search practices of TSA officers that lead to this experience. A screener squeezed the urostomy bag of the passenger, which leaves an impression of rudeness but also blindness on the part of TSA officers as the indication provided by ATR software reveals no information on the type of an anomaly for the responsible officer. Mr. Sawyer addresses the TSA's behavior in stating that he sees a real disconnect between what they say they are doing and what is really happening at the airport. With this statement the passenger addresses problems that are related to the instruction of TSA officers using ATR software appropriately. In answering some of the criticism that has been raised by indignant passengers the TSA has responded to criticism. TSA's John Pistole talks about the agency's position in the *NYT*:

> He said they are trying to move past a "one-size-fits-all" program and implement a "risk-based, intelligence-driven process" by the end of the year that would have more refined targeting. If passengers are willing to share the same information they give to airline frequent-flier programs, he said, maybe some day they will be able to "keep their jacket on and their laptop in their briefcase and hang on to that unfinished bottle of water. "I'd like to get to the point," he said wistfully, "where most people could leave their shoes on" (NYT, 2011: SD 27).

John Pistole talks about moving past a "one-size-fits-all" program. In saying so he acknowledges to some degree that the conception of a "standard body" remains problematic.

Although this shift in opinion appears compelling, Pistole basically avoids talking about the physical distress passenger experience with pat-downs. In that sense attention is shifted away from the body to the promise of benefits (keeping jacket, bottle) that have nothing to do with the body. Pistole wants to achieve this through a “risk-based, intelligence-driven process” along with more refined targeting. The TSA administrator implies that this means an endeavor that is connected to giving up on security in some cases by shifting attention to places of greater interest and foregoing areas that are regarded as being rather safe. Pistole makes some concessions but also connects them to the need for passengers to share more information. This move turns the passenger into an important actor in the intelligence-driven process. The TSA administrator gives a weak promise of regaining former conveniences at airports but also asks for a mutual exchange of commitments. Pistole declares that it is his intention to reach this point in the future.

Whereas the TSA sees the software as subordinate to the work of TSA officers (SD 23), the opposite view can be found from examining other stakeholder documents. The general tendency of stakeholder documents sees TSA officers as lacking tact (SD 24,25,26). They portray TSA officers as ignorant, lacking in sensitivity and sticking to an exact screening procedure. Many of the complications turn out to have a detrimental effect on the work of TSA officers. The human-machine interaction brings several flaws with it but most obviously all problematic aspects that stem from the collaboration are regarded as failures of human workers. In one example a commentator on regulations.gov (SD 22) argued that technology further separates passengers from staff and hence have egative effects for passengers under scrutiny. With exception of the TSA all other stakeholders conceive the work of TSA officers as having a negative effect on security screening. This development comes as a surprise and citizens also seem to have problems following what exactly goes wrong when ATR software and TSA officers work hand-in-hand. As one indignant passenger noted: "I just don't understand why it's so difficult to train these agents" (SD 28). Much of the one-sided depiction on how conceptions on security in this scenario are made becomes apparent. With respect to the criticism, the TSA’s proposes a “risk-based” approach (SD 27) and a more nuanced treating of passengers. However, alterations to the screening process are tied to the disclosure of more information from passengers.

Coming back to the research question “How does the application of ATR software affect the perception of TSA officers' work?”, it is concluded that ATR software has a negative effect on the perception of how TSA officers approach the body of the individual passenger. Interestingly the stakeholders see the main problem not in the technology of ATR software

but rather in the training efforts of TSA officers to make use of the technology. In that sense the application of ATR software is perceived as being misleading and not properly adopted by the agency. While passenger experience harsh controls through TSA officers, ATR software remains untouched from critics. This is surprising as ATR software commences the detection process that leads to an enhance pat-down on a passenger. While the TSA acknowledges offensive controls it relates easing of the screening process to the disclosure of more privacy related information of the passengers. As this chapter has foremost been concerned with the role of privacy it is argued that the TSA perceives privacy once again as not presenting a basic right of passengers. Passengers can expect easement of controls only when they are willing to waive on privacy and share even more information with the agency.

5.2.3. A discourse of enhancing privacy

The present chapter illustrates a more abstract analysis of the **subchapter RQ4: How do stakeholders portray the effects of ATR software on passenger privacy?**

The introduction of ATR software has been accompanied by a discourse on enhancing (SD 17-20) and/or further enhancing (SD 15) privacy (SD 21). The notion of enhancing privacy was first mentioned in 1995 when the term “privacy-enhancing technology” appeared as the title of a governmental report (Office of the Information and Privacy Commissioner of Ontario [OOTIAPCOO], 1995). Basically Privacy Enhancing Technology (PET) is defined as:

> ”a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system” (Blarkrom, et.al., 2003: 33).

In applying this notion to ATR software the definition of PET only seems to partially comply. As it has been mentioned before the graphical display of ATR relies on the same data that AIT scanners obtain from the body of a passenger. ATR software in that sense neither eliminates nor minimizes the data taken from a passenger. If anything the definition of ATR promises a possibility to visually obscure the apparent information retrieval of the passenger. The Privacy Commissioner of Ontario has further developed the conception of PETs to PETs Plus, creating the new concept of Transformative Technologies. Being dissatisfied with a “zero-sum” paradigm where gains in security or privacy always mean an impairment of the other, Transformative Technologies rely on a paradigm of “positive-sum”, making every party benefit from advances in technology (Cavoukian, 2009a). The notion of Transformative Technologies is further explained in another document from the office:

> ”Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance structures” (Cavoukian, 2009b: 1).

Despite the utterly positive conception of PETs the TSA’s attempt to promote public confidence is also seen in the introduction of ATR as a correction to previous screening procedures. ATR software represents an approach to answering privacy problems via a “technological fix” that quite often results in ineffective and unsustainable results (Robins & Webster, 1989). Whereas societal trust in the “technological fix” has been undoubtedly established (Weinburg, 1966), raising the problem of invasive AIT scans a “technological fix” is enacted to lower the outrage and appease those who feel offended. This procedure of harming privacy and then partly restoring it is represented as an “enhancement” to privacy, a beneficial outcome for everyone. Despite the positive rendering, privacy is severely damaged by means of a technological invasion of depicting and condemning individual vulnerabilities and characteristics on passengers who do not correspond to conceptions of ‘normal’ body. This tendency of applying AIT and “improving” it through ATR is reminiscent of a mentality of technopositivism. Thus, “if you have a problem, define it in terms of information and you have an answer.” (Brown & Duguid, 2000: 19).

5.2.4. A discourse of incompatibility between man and machine

The present chapter illustrates a more abstract analysis of the **subchapter RQ5: How does the application of ATR software affect the perception of TSA officers' work?**

Concerning the actual screening processes stakeholder documents report on a series of misunderstandings that result in a lack of sensitivity and passengers’ being greatly offended (SD 24,25,26). These recurring mistakes emphasize the assumption that there are several difficulties in adjusting the operational procedures between human and machine interaction. In the case of ATR software, which due to privacy related reasons only provides limited visual information, human-machine communication appears very restricted. It remains highly questionable in how far a TSA officer can make reliable assumptions about a possible threat from the depiction of a box on a generic outline. As stakeholder documents have shown ATR becomes an impractical piece of software that contrary to TSA declarations (SD 23) does

little to help the TSA officer to determine with what kind of anomaly human workers has to deal:

> "The severe limitations on the informational resources available to the machine – basically changes in its state mapped on to a priori assumptions about a user's projected course of action – correspondingly limit the machine's ability to engage in anything like the subtle, emergent, and highly contingent courses of collaborative sense making that characterize interaction among humans" (Suchman, et al., 1999: 395).

As a consequence the concessions that have been made by the TSA to answer privacy concerns are an attempt to reduce uncertainty and humiliation at ATR controls. Hence the distance that is created between passengers and TSA officers is further emphasized through improving throughput capability of the scanners (SD 15, 17-20) as well as a desire to streamline the checkpoint screening process (SD 17-20). As one of the main challenge of today's airports is to both maximize and regulate mobility (Salter, 2007) time remains a scarce resource, which requires the detection process to accelerate and become automatized. In addition, the continuing growth of worldwide air traffic demands uncomplicated and streamlined controls. Passenger air traffic continues to grow and jumped from 2009 to 2011 by 14.8 percent (Berster, 2013). Whereas early AIT screenings included a second TSA officer who was delegated to inspect the naked body images of passengers, the need for this kind of human operator has continuously been neglected by the TSA when referring to the introduction of ATR software. Despite privacy concerns, the second TSA operator was able to view the complete body of the passenger with all its body shape characteristics. Thus human judgment and conversation supported and more importantly instructed the TSA officer at the checkpoint on how to approach the passenger and which regions of the body were believed to carry a potential threat or were in fact the site of bodily characteristics that had to be encountered carefully. As this possibility has been lost in the new ATR process design the TSA officer must rely solely on the graphical output of the software that shows nothing more than a box and gives no further feedback to determine the type of detection. Suchman argues, "conversations among people succeed not because of the absence of troubles in understanding, but rather due to a wealth of resources available for their collaborative identification and repair" (Suchman, et.al., 1999: 395). This highlights a particular feature of ATR, namely that it does not allow for nuances: it remains restricted to operated using black-and-white categories of dangerous and secure and, due to privacy implications, cannot free itself from this restriction and draw on human inspection and intelligence. Curiously the little information given reflects poorly on the work of TSA officers

as a lack of understanding is attested in misguided training efforts (SD 28). This is seen as another proof for the strong impact of mechanical objectivity (Daston & Galison, 2007). that not only plays an important part in the detection process, but also affects the work of TSA officers. Passengers do not question the conception of the scanner with ATR software and even more curiously are annoyed by TSA officers that follow the instructions of the devices.

5.3. On the generic outline and the display of the human body

Concerning the third and final section of the analysis, the focus moves to the visual representation of the passenger. Whereas the first two sections gave impression of detection, anomaly, privacy, efficiency, and human-machine interaction the third section is primarily concerned with the form of the visual depiction as mentioned in the stakeholder documents. As a major concept of the software the generic outline represents the visible alteration to the software upgrade. In February 2011 the *NYT* writes about the fundamental change in display that is achieved through the introduction of ATR software:

> In response to concerns about the body scanners, the agency last week demonstrated software it was testing at Las Vegas McCarran International Airport that allowed the machines to display a generic outline of a human figure rather than the graphic images some passengers view as a privacy invasion (NYT, 2011: SD 29).

The display of ATR software resides at the foreground and communicates meaning to the TSA officer as well as the passenger. The depiction is also what is commonly understood as a user interface, conceiving the "means in which a person controls a software application or hardware device. A good user interface provides a "user-friendly" experience, allowing the user to interact with the software or hardware in a natural and intuitive way. (Techterms, 2013). Intuitive in that sense means that it becomes self-evident how the software represents predefined capabilities of a machine. Most of all, this understanding is integrated into ATR software through the depiction of a generic outline: "ATR is software that's used with Advanced Imaging Technology (AIT) and displays a computer generated, generic human image (you've probably heard it referred to as an Avatar) on the monitor attached to the AIT machine" (Burns, 2010b). In using the notion of an avatar, the TSA indicates that the individual passenger's body is shown through a human body integrated into the display of ATR software. An avatar denotes "an icon or figure representing a particular person in a computer game, Internet forum, etc." (Oxford Dictionaries, 2013c). However, the display of the human body has not only been the key characteristic of recognizing the human within the depiction of software, it also has contributed vastly to concerns over the individual privacy of passengers. The unintended dissemination of individual photographs deeply undermined the trust in the TSA:

> Yet the leaking of these photographs demonstrates the security limitations of not just this particular machine, but millimeter wave and x-ray backscatter body scanners

> operated by federal employees in our courthouses and by TSA officers in airports across the country. That we can see these images today almost guarantees that others will be seeing similar images in the future. If you're lucky, it might even be a picture of you or your family (Johnson, 2010).

The article, which appeared on the tech blog Gizmodo, refers to security limitations that almost guarantee the spreading of images. The depiction of an individual passenger is generally regarded as an action that can bring along many problematic revelations. In order to emphasize that the same mistake will not be made again, the TSA points out that ATR software is simply not able to generate permanent pictures: “ATR-enabled units are not capable of storing or printing the generic image produced during screening” (Sanders & Cantor, 2012: 5). This sentence is interesting insofar as it removes any connection to the image of the individual body of a passenger. The authors testified before a Homeland Security Subcommittee that pictures taken by AIT are by nature generic. As there is only a generic image available privacy concerns turn out to be redundant. The inability to store or print pictures confirms this kind of double insurance: the images are made harmless in the first place and in a second step modifications are taken up that block further distribution. Consequently this is also where the reference to the notion of the avatar comes full circle. Any reminder of the individual passenger has somehow disappeared and everything that is left is represented through a generic outline in the shape of an avatar. The way in which the human body is displayed seems to be of great importance for the TSA. At one point the agency develops the thought of letting the individual disappear even further: ”This past summer, we rolled out new software on all of our millimeter wave units so that all we see on these units is a generic outline of a person. And that’s only if the machine detects an anomaly” (Burns, 2011b). What the official TSA Blog says in this statement is that in case of no detection the ATR software displays no generic outline of the passenger. One can also read from this commitment that the display of the human body in any form is a delicate task that easily calls attention to privacy concerns. As a consequence the research question states:

Subchapter RQ 6: How do stakeholders portray the approach of ATR software to depicting the human body with a generic outline?

The TSA writes in one of the agency’s newsletters on concerns of the individual:

> In the coming months, TSA will install the software upgrade on all currently deployed millimeter wave imaging technology units at U.S. airports nationwide. By eliminating the image of an actual passenger and replacing it with a generic outline of a person

> passengers are able to view the same outline that the TSA officer sees (TSA, 2011: SD 30).

TSA claims that the software upgrade will bring dramatic changes to the screening process. The TSA uses the strong expression of 'elimination' to emphasize that images of passengers are once for all removed from the search. Elimination means not only that all future display of the human body is extinguished, but also that every reminder of the human body is transformed into a standard depiction, which represents yet another way of normalizing the body. Most likely this is also tied to concerns on the processing of data material that became apparent through the leaking of passenger images. The TSA reinforces this strong commitment in following up with a statement on mutual transparency. In stating that passengers are able to view the outline of themselves, the agency suggests that it has nothing to hide. Basically, the agency grants its passengers the ability to gaze on the software output and puts passengers and TSA officers on the same level. This is regarded as a positive move towards passengers that brings them and TSA officers closer together and provides for an encounter on equal footing. Before the use of a generic outline, the responsible for validating anomalies received audio-commentary by a second officer, who examined pictures of the passenger in a separate room. Whereas the screening procedure before ATR only enabled the remotely located TSA officer to view pictures of the individual, the introduction of the software has changed this. With ATR both the passenger and the TSA officer view the same picture, an alteration that is used to regain confidence in the system. In a similar manner the use of a metaphor for elimination is also found in an article from *The New York Times*, describing a vivid picture of a crime-scene.

> Rather than displaying the image of an individual's naked body, the L-3 machines depict any foreign object on a person and display only a generic body outline, similar to the police chalk outline of a body at a homicide scene (NYT, 2013: SD 31).

The article compares the shape of a generic outline to a police chalk outline at a murder scene. The picture invokes thoughts of both the disappearance and elimination of an individual human body. A chalk outline points to the location where the victim lay prior to being removed from the crime scene. This disappearance of the body is also found in the statement from the TSA (SD 30). Nevertheless, newspaper's example also evokes the impression of the passengers as being victims. Commentators on regulations.gov also see the human body as disappearing, although in a weakened form: "I am under the impression that all you see now is a stick-figure. If that is in fact the case that is ok. Anonymous" (Regulations.gov, 2013: SD 32). Arguably it is of greatest importance for the citizens what

can be seen with the naked eye. The use of the notion 'stick-figure' has been prominent within the media as a way of describing the general outline. Still, the commentator is not entirely sure what representation of the human is used at ATR controls. In another TSA statement the generic outline receives another attribution. While referring once again to a notion of disappearance, the second focus lies with a unified depiction through ATR software:

> The new software will automatically detect potential threat items and indicate their location on a generic outline of a person that will appear on a monitor attached to the AIT unit. As with the current version of AIT, the areas identified as containing potential threats will require additional screening. The generic outline will be identical for all passengers. If no potential threat items are detected, an "OK" will appear on the monitor with no outline (TSA, 2011: SD 33).

The agency states that the generic outline disappears when no threats are detected and leaving nothing more than an "OK" sign. In that case the passenger completely dissolves from the screen attached to the AIT scanner. They argue that the body is of no more interest for the TSA, while it still remains in place although in a normalized form. The second observation contains a statement that builds common ground among passengers. As the TSA declares that the generic outline will be identical for all passengers, every reminder of individuality is taken from the statement. Superficially it seems the agency no longer keeps an interest in the depiction of the individual passenger while AIT scanners still continue to create invasive pictures of passengers.

5.3.1. Equal vision

Whereas the first statements of this section were mainly concerned with the state of depiction of the individual passenger, stakeholder documents also share a second similarity across the board. In the TSA's first statement the agency already referred to the ability of equal vision between TSA officers and passengers (SD 30). This observation has also found its way into a *New York Times* article, where the introduction of a computer screen is highlighted:

> The T.S.A. has also installed new software on certain body scanners designed to improve privacy by replacing the virtual nude images of passengers, previously used, with a generic, computer-generated outline. Passengers are now able to view the same image online that the security officer sees on a computer screen as they pass through security (NYT, 2011: SD 34).

In referring to the ability of passengers to share vision with a TSA officer on a monitor, this step is regarded as improving passenger confidence. In sharing its view, the agency allows the passenger to also take part in the security-screening process. This is a direct appeal to passengers to get involved and actively take part in screening. As a benefit of this procedure the passenger can possibly give insights on any potential detection discovered on his or her body. The passenger thus becomes an accomplice in handling security checks with ATR. EPIC also makes a point on this newly gained ability that is provided through ATR software:

> The Transportation Security Administration (TSA) has announced that it will begin installing new software on some millimeter-wave airport body scanners that will display a generic human figure on a computer monitor rather than the naked bodies of individual air travelers. Passengers will be able to view the same images as TSA employees (EPIC, 2011: SD 35).

The organization sees the display of a generic human figure instead formerly naked bodies of individual air travelers as an improvement. The ability to simultaneously see pictures made by ATR software can be read as a metaphor for looking over the shoulders of TSA agents. Even more importantly, the passenger becomes actively involved in the screening process. As a consequence the statements of both the *New York Times* and EPIC lead to a general impression that is verbalized by TSA administrator John Pistole in *USA Today*: Allowing travelers to see the monitor will give the public "greater confidence" in the system and serve as a deterrent, Pistole said (USA Today, 2011: SD 36). This statement foremost has to be regarded in the context of the many leaked pictures that have caused tremendous insecurity among citizens. To finally be able to ‘see’ how technology works and what it achieves is regarded as a step toward regaining trust in the agency and consequently the technology used. The TSA claims that this is a move towards more transparency insofar as it actively invites passengers to see how the TSA handles security work.

The discourses concerning the introduction of a generic outline can be separated into two categories. Whereas the first emphasis falls on the disappearance of the individual body, the second focus lies with the ability to share the view on the actual process of screening. Stakeholder documents portrayed the generic outline foremost in terms of a disappearing or elimination of the individual human body (SD 30-35) from the control process. The replacement of the individual passenger takes place through an outline that is identical for all passengers (SD 33). As a consequence some stakeholders emphasize the ability to view the same pictures as TSA officers (SD 30,34,35).

Coming back to the research question, “How do stakeholders portray the approach of ATR software to depict the human body with a generic outline?”, two answers have to be given.

With respect to the depiction of the body it is claimed that the image of the individual human body has disappeared completely and therefore memories of naked bodies are a thing of the past. Secondly, the stakeholder documents declare that there is now the possibility to view the exact same images as TSA officers do. The display of the human as a homogenized being with a standardized body depiction further serves the construction of an expected body shape. There appears to be only one correct depiction on the computer screen where ATR software is displayed and passengers need to conform to this depiction or else they become the subject of an enhanced pat-down.

5.3.2. A discourse of filtering concerns

The present chapter illustrates a more abstract analysis of the **subchapter RQ 6: How do stakeholders portray the approach of ATR software to depicting the human body with a generic outline?**

With respect to discourses on the depiction of a generic outline, stakeholder documents have continuously used the notion of eliminating the image of an individual (SD 30-35). Among the discourses it is perceived that it has become impossible to see the individual and that reference to the human individual can no longer be achieved since the introduction of ATR software. However, the passenger remains positioned in the AIT screening device and nothing has changed in the process of scanning the passenger via the use of millimeter wave technology. As the visual display seems to be of great importance, the metaphorical discourse of a filter has been attested. ”TSA implemented “chalk outline” filtering, known as a privacy algorithm, to allay privacy concerns, as raw, unfiltered X-ray backscatter images resemble high- resolution photographic negatives” (CRS, 2012: 2). Most importantly for applying the metaphor of a filter is that empirical reality is always complex than what people perceive and experience. Things in the world in that sense exceed any and all filtered perceptions thereof (Friedman, 2011).

That which remains “noteworthy” for the TSA is presented as a generic outline with no personal details of a human whatsoever. “Noise” then refers to all the very important details that are relevant for detection and consequently examined through the AIT scanners but ultimately remain in the background. Hence, the introduction of a visual filter allowed the TSA to discursively eliminate the actual picture of the passenger to a degree that he or she cannot be recognized anymore. If everything that remains to be seen is equivalent to a stick-figure (SD 32) then concerns are swept away. While the applying of a filter on top of images might soothe visual concerns, the elimination of individual images goes beyond allowing the public

to forget pictures of their naked bodies. “A criticism of blurring or obscuring is that this objectifies people and removes their identity. Without faces people appear not as people at all but as objects” (Wiles et. al., 2008: 23-24). In that sense protective measures to obscure the display of naked bodies turn into general assumptions of an objectified body whose unique characteristics seem to be of no concern.

5.3.3. A discourse of building trust

The present chapter illustrates a more abstract analysis of the **subchapter RQ 6: How do stakeholders portray the approach of ATR software to depicting the human body with a generic outline?**

The ability to see equally has been continuously mentioned in stakeholder documents (SD 30,34,35). To share equal vision also fosters confidence among individuals as it allows strangers to rely on a common ground. Popular sayings such as “I saw it with my own eyes”, to “seeing is believing” or “a picture is worth a thousand words” understate the importance of vision, far above other senses. Concerning ATR software it remains important to ask what kind of empirical reality is created here. The perceived reality of “What you see is what you get” is rendered alive and thus becomes “real” through a friendly outline on the screen for the TSA officer and the passenger alike. However, there are also contrary perceptions of the depiction that have been associated with the chalk outline of a victim at a crime scene. Formally, lost trust is regained by the TSA in displaying openness and the possibility of sharing the view. Of course, one should not forget that the setting at airport screening points still remains one with clearly attributed roles, namely the passenger under scrutiny and the TSA officer in the position of power. Nevertheless, ATR software has discursively been rendered as a way to regain trust and “greater confidence” (SD 36) through the act of being able to view the monitor on an equal basis. Whereas AIT controls remain as invasive as ever and create pictures that can detect anomalies in regard to a standardized body conception, the discursive realization and its technological equivalent represented through ATR software tell a different story. As a consequence, the possibility to view the monitor as the TSA officer does is regarded as a sign of building trust by the agency towards the traveling public. It is essentially an invitation to share the same mutual view on a monitor and thus to take part in this mutual effort to guarantee security and also in enabling a quick screening process. That being said, trust still remains a generous way to describe what Pennings and Woiceshyn regard as a “mode of control” (Pennings & Woiceshyn: 1987: 85), one that allows for the

continuation of invasive practices while at the same time making passengers feel that they are in control of the screening process and in so doing see their privacy concerns dissipate.

6. Discussion and results

How does a surveillance technology such as AIT with ATR affect and transform perceptions of privacy and security?

The discourses have been attested on three different levels that correspond to the chapters of analysis.
The detection ability of ATR software has continuously been rendered by the TSA as having a very concrete ability to detect threats. In general, the TSA constructed a continuing and carefully shaped rhetoric of threats and insecurity within their statements. There is also emphasis put on the technology's capability to detect even the smallest threats and ATR is furthermore presented as a future-proof solution. While threats are permanently mentioned and vigilance is required from every citizen, deployment of technology is regarded as a necessity. As new threats of fluids, powders, and plastic explosives appear, society is required to respond with new technical solutions that deter terroristic attacks. For example, ATR is labeled as a counterterrorism tool that also allows for the detection of powders and other dangerous substances.

Overall, the discourses applied by the TSA center around perpetual risks and terrorist threats that construct an atmosphere of "fear" (Furedi, 2002),
Hence, security measures applied also build upon the continuous increase of fear and potential ways to harm society. Fear becomes instrumentalized and becomes a variable that must be controlled. According to Furedi "through risk management, fear is institutionalized", which conveys the presumption that "fear response is further encouraged and culturally affirmed" (Furedi, 2007).

Efforts to manage future threats thus demand that threatened citizens and the nation as a whole close ranks. National identity is constructed by discussing the evil forces that try to wound American values through devious attempts of bringing death past airport security. The TSA, for its part, claims to ensure the security of the traveling public, while also constructing the potential risk that lies within every passenger and urging every citizen to remain vigilant at all time. As everyone represents a potential risk there is no end to the application of ever-

new security measures in sight. The obligation to submit one's body to screening remains a small price to pay for keeping the deviant "other" out of reach of their loved ones. The continuous fear of the faceless "other" that lurks somewhere out there for a chance to hurt the US leads to a fear of crime that Bannister and Fyfe regard as "a more widespread problem than crime itself" (Bannister & Fyfe, 2001: 808).

While the discourses realized by the TSA remain stark in their one-sidedness, there have also been attempts made to contest the depiction of ATR as a profound detection tool. Comments from regulations.gov as well as EPIC deny the ability to detect objects, with statements in both cases pointing to AIT's restriction of only revealing anomalies, many of which are false positives. Likewise, contradictions regarding the materiality of an anomaly are also discursively raised by EPIC and regulations.gov. Both stakeholders effectively deny the assertion that AIT is capable of detecting threats such as powdered explosives that have been presented as a stand-out feature of AIT in comparison to metal detectors.

With respect to inconsistencies in the detection process neither newspaper went so far as to deem AIT incapable of detecting threats of non-metallic origin. Instead, *The New York Times* and *USA Today* portray the experiences of several passengers whose bodies were marked as anomalous – running afoul of ATR's conception of a normal body – and thus seen as a potential threat. Nevertheless, this criticism appears to be somehow softened. While the newspapers portray ATR as being potentially invasive with regards to the bodies of certain passengers, they do not question its general detection abilities. In contrast to the depictions drawn by EPIC and comments on regulations.gov, the view of the two newspapers seems to be that while the software's instrusiveness may seem harsh, it gets the job of detection done.

As the controversy over the procedure continued, the TSA also made several small concessions that were related to efforts in getting smarter about security and easing the screening process for the very young and very old. However, despite criticism the screening method has not been altered in any way.

Despite concerns by the media and public outrage, the introduction of ATR software has been realized not only solely in response to privacy deliberations. The need to continuously introduce new technologies to security screening processes (TSA, 2013b) as well as escalating TSA staff costs (SOTSCOHS, 2012) provided further impetus for the use of ATR. The perception of ATR software is regarded across the board as a positive alteration to the screening process. ATR is discursively realized as a beneficial package that, besides enhancing privacy, also constructs an imagination of improved throughput capabilities, a streamlined screening process, and, overall, the idea of an uncomplicated, almost

convenient screening process that is free of any invasive touching. Controversies around privacy implications of ATR software remain negligible. Whereas claims of a more straightforward screening process were not incorporated or contradicted, with one exception on regulation.gov claiming increased efficiency, privacy alterations were the most salient topic.

The agency claims that the measures it has taken have enhanced privacy protection, an aggressive discursive strategy that defends the former practices of AIT controls as a just examination of the human body. As citizens become used to invasive practices they are afterwards pleased with the means of a "technological fix" (Weinberg, 1966), resulting in the promotion of public confidence (Cavoukian, 2009b). The betterment of a questionable status obviously possesses the ability to create relief in the perception of stakeholders. As *USA Today* claims that passengers will receive more privacy, so a commentator on regulations.gov regards ATR software as an improvement of privacy, previous bad experiences with AIT are seen once and for all as things of the past. Responding to the public outrage that from the beginning centered more on the depiction of the body than on the scanners' performance, the TSA continuously applies a 'carrot-and-stick' strategy by which it enacts and then later scales back drastic encroachments to please the public and news media. This is basically the same strategy that was used by the TSA in easing screening for very old and very young passengers.

Concerning the interaction between scanners and TSA officers a different picture emerges. Whereas the TSA conceives ATR as an ideal aid to TSA officers, the software appears to be disadvantageous for TSA officers in daily work routines. Beyond that the application of ATR leads to a general dissatisfaction that is projected onto the work of screeners. While the human screener is regarded as a potential source of errors, emphasized by comments on regulations.gov, scanners appear to be just in their efforts of deciding who should pass and who should be subject to further scrutiny. ATR software in that sense stands as an immovable machine, to which practices need to be adapted. It takes over human judgment with no room for an interpretation and reduces TSA officers to mindless executors who arouse anger of the flying public. The discursive promises that are made through accelerated checkpoint processes result in an incompatibility between man and machine that is increased by restricted information provided through ATR (Bellanova & Fuster, 2013) and further pushed by augmenting visitor streams (Berster, 2013). TSA officers appear in discourses concerned with their performance as inadaptable to objections and indications made by passengers. The work of TSA officers carries a roughness that lets the human appear as the most impersonal link in a chain of checkpoint security. Paradoxically, with the advent of ATR

software the privacy of passengers seems no longer to be threatened by technology but rather by rudeness on the part of TSA officers. The discursive patterns located ultimately point towards a further substitution of human workers through technology.
Interestingly, after negative media coverage the TSA agreed to make some concessions to the traveling public. As a repeating pattern these compromises present only little relief (e.g. the possibility to leave shoes or a jacket on) and were in this case projected to an unknown point in the future.

The depiction of a generic outline on ATR software represents the most obvious alteration to AIT so far. Most interestingly, stakeholder discourses resulted overall in great conformity and dispute has not been attested. The display of ATR software has strong implications on the perception of the individual self and, as images are believed to make meaning, (Hall, 1997) stakeholders willingly recycle discursive efforts by the TSA. The discursive realization by the TSA surrounded two important features that were continuously redistributed.
The first discursive argument concerned the depiction of ATR software and declared that any resemblance to the individual has been eliminated. Stakeholders agree that the depiction stands for a human prototype, an abstract avatar serving as an inoffensive two-dimensional placeholder. As the invasiveness of naked pictures remains obscured, concerns about the scrutinized surface of the body also disappear. Notably, EPIC also assimilated this discourse with no criticism whatsoever as the NGO accepted the change that the individual is replaced by a generic image. Using the generic outline has become a no-brainer that has been taken up uncritically by every other stakeholder. Only in one case *The New York Times* compared the outline to a body at a homicide scene, likening the victim there to a passenger during the screening process. Besides this single exception, commentators on regulations.gov have broadly welcomed the effect of a filtered depiction. A filter, it seems, is sufficient to settle concerns that were previously associated with the depiction of the human body. The perception of privacy therefore is manifested on the obvious things people can see (Kula, 2011). Through obscuring past experiences of offensive pictures the filter repaints the depiction of the individual. It replaces the uncomfortable with the indifferent. It pleases our consciousness while enabling continuous operation in the dark. Attwood and Lockyer emphasize the importance of images as they mark “key areas of dispute and act as reference points for social, cultural, and political arguments” and are “increasingly becoming the signs and symbols of major contemporary concerns – often centered on sex and sexuality, political and religious conflict, … and the boundaries between the public and the

private" (Attwood & Lockyer, 2009: 1). It seems that along with the ability to see the generic image concerns about the depiction of naked bodies inside of scanners also begin to vanish.

The second feature referred to the ability to view the same pictures as TSA officers do, a move that promoted the role of the passenger from a suspect to an informed participant in the control process. Whereas passengers previously had no indication whether they posed a threat, ATR software promotes the passenger to the role of accomplice to TSA screeners and makes them an informed part of the screening process.

As TSA efforts carry transparency in their discursive realization, trust in the agency is restored. This discursive uptake by stakeholders is interesting insofar as the TSA effectively obscures the procedure of screening passengers. Thus, both passengers and TSA officers see the same depiction, while they ultimately do not really see anything. The information provided by ATR software is reduced to the location of a potential threat but it seems to work as an indication of what to expect from the screening process. ATR functions as a "mode of control" (Pennings & Woiceshyn, 1987: 85) that projects trust and confidence towards the passenger.

Still, along with the depiction of a generic outline the reference to the real body is lost, whether passengers are standing inside a cabin or not. The work that is achieved through AIT and ATR software reduces the body and obviously also the perception of the body to a plain object that has no longer any relationship to bodily privacy (Wiles et al., 2008). The human understood as an object is not interested in what is happening inside the scanners. He enters into an apathetic state in which he accepts every intrusion, however dramatic, into his private realm. The representation through ATR software is the promise by the TSA to care for its passengers. It represents a gesture toward passengers that defuses obvious concerns and, in turn, obtains virtually complete acceptance. ATR software is able to turn around the negative perception surrounding AIT. Much of this effort can be related to the visual display that took an isolated screening room and allowed it to be openly shared with passengers.

The controversies that have been attested in this discourse analysis show something important in terms of technology development. As technologies become inherently hard to look through criticizing them also becomes a difficult task. The unobtrusive nature of ATR software makes it hard to scrutinize the scanners; more than once such criticism has resulted in the takeover of discursive strategies from the TSA. Scholars refer to this phenomenon as the "silent nature of information technology" (Introna & Wood, 2004). ATR exemplifies the trend of technology to move more and more into the background. No resemblance to the individual shall be possible and, thus, concerns also disappear, as people do not understand

what is happening to their bodies. The human turns into an object as the body becomes the means of identification. As risks have to be minimized, checks have to rise with difficult consequences for everyone who does not have a “normal” body according to TSA’s definition.

While it has been shown that language shapes views of conceiving the world, pictures that are placed on top of ATR software seem to reach agreement even more.

The application of discourse analysis has proven to be generally a good means to trace strategies and perceptions of stakeholders. As Abe attested, when the government encounters little resistance from the media (Abe, 2004) stakeholder discourse analysis helps by integrating other actors and bringing their (new) views onto the agenda. In that sense it remains important to mention that only EPIC and regulations.gov directly criticized the detection capabilities of ATR software. Among others this example also supports the integration of a broader base of stakeholders with different backgrounds.

Future scenarios of AIT use point to a broader introduction in society to come. AIT is today already used to create neoprene wetsuits that perfectly fit the body of a swimmer (Bodyscanningcrm, 2013). Other scenarios allow the adjustment process of various appliances, from chairs, to bicycles, or tailored running shoes. In consumer society AIT provides an impressive ability that abandons mass production towards unique, made-to-measure products for the individual.

With respect to surveillance, a concept for the FIFA Football World Cup 2022 declares, “full body scanners represent the main security gate control technologies. They are complemented by smart scent sensors that are able to detect even single segregated molecules of explosives such as TNT or pyrotechnic materials. Additionally, these sensors have also the ability to give warning about somebody who is carrying drugs or who is drunk” (Friedewald & Wright, 2012: 4). As AIT is believed to gain further momentum, the general retreat of surveillance technologies from the perception of citizens also seems to carry on. This thesis has been an effort to point towards the implications that can stem from the means of mitigating and hiding the obvious in technology. While this has been a first attempt to comprehensively outline and grasp the implications of ATR, more detailed research is needed to consolidate the attributions of the effects of the software on the perception of passengers.

7. Literature

'The New York Times' n.d., *Wikipedia,* wiki article, viewed 28 December 2013, http://en.wikipedia.org/wiki/The_New_York_Times

'The Public Voice' n.d.: *Case Study: Electronic Privacy Information Center (EPIC).* Viewed 28 December 2013, http://thepublicvoice.org/events/EPIC_Case_Study2.pdf

'USA Today' n.d., *Wikipedia,* wiki article, viewed 28 December 2013, http://en.wikipedia.org/wiki/USA_Today

Abe, K (2004): *Everyday Policing in Japan: Surveillance, Media, Government and Public Opinion.* International Sociology, vol. 19, no. 2, pp. 215-231.

Agre, P (1995): *Conceptions of the user in computer systems design.* In: P, Thomas (ed.), The social and interactional dimensions of human-computer interfaces. Cambridge University Press, New York.

Ahlers, M (2010): *Additional airports to get full-body scanners, feds say.* CNN.com, viewed 27 December 2013, http://edition.cnn.com/2010/TRAVEL/03/05/body.scanners.airports/

Allen, A (2011): *Unpopular Privacy: What Must we hide?* Oxford University Press, New York.

Amendment IV (1791): Fourth Amendment. Law Cornell.edu, viewed 28 December 2013, http://www.law.cornell.edu/constitution/fourth_amendment

Ammicht, QR; Rampp, B (2009): *It'll turn your heart black you can trust: Angst, Sicherheit und Ethik.* Vierteljahreshefte zur Wirtschaftsforschung, vol. 78, no. 4, pp. 136-149.

Anthony, L (2012): *AntConc (Windows, Macintosh OS X, and Linux) Build 3.3.5.* Antlab.sci, Viewed 28 December 2013, http://www.antlab.sci.waseda.ac.jp/software/antconc335/AntConc_readme.pdf

Armstrong, G; Norris, Cl (1999): *The Maximum Surveillance Society: The Rise of CCTV*. Berg Publisher, Oxford.

Attwood, F; Lockyer, S (2009): *Controversial Images: An Introduction.* Popular Communication: The International Journal of Media and Culture, vol. 7, no. 1, pp. 1-6.

Augé, M (1995): *Non-places: Introduction to an Anthropology of Supermodernity.* Verso, London.

Ball, K (2005): *Organization, surveillance and the body: Towards a politics of resistance.* Organization, vol. 12, no. 1, pp. 89-108.

Bannister, J; Fyfe, N (2001): *Introduction: Fear and the city.* Urban Studies, vol. 38, no. 5/6, pp. 801-813.

Bannon, L (1991): *From human factors to human actors. The role of psychology and human-computer interaction studies in system design.* In: J, Greenbaum; M, Kyng (eds.), Deign at work: Cooperative design of computer systems. Erlbaum, Hillsdale.

Barnard-Wills, D (2011): *UK News Media Discourses of Surveillance*. The Sociological Quarterly, vol. 52. no, 4, p. 548-567.

Bauer, MW; Bonfadelli, H (2002): *Controversy, media coverage and public knowledge.* In: MW, Bauer; G, Gaskell (eds.), Biotechnology – the making of a Global Controversy. Cambridge University Press, Cambridge.

Beck, U (2009): *Critical Theory of World Risk Society: A Cosmopolitan Vision.* Constellations, vol. 16, no. 1, pp. 3-22.

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

Bellanova, R; Fuster, GG (2013): *Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices.* International Political Sociology, vol. 7, no. 2, pp. 188-209.

Berger, PL; Luckmann, T (1969): *Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie.* Fischer, Frankfurt am Main.
Berster, P (2013): Luftverkehrsbericht 2011 ist erschienen. DLR.de, viewed 29 December 2013, http://www.dlr.de/fw/desktopdefault.aspx/tabid-2937/4472_read-36027/

BeVier, LR (1995): *Information About individuals in the hands of government: Some reflections on mechanisms for privacy protection.* William and Mary Bill of Rights Journal, vol. 4, no. 2, pp. 455-506.

Bigo, D (2006a): *Globalized (in)Security: The field and the Ban-opticon.* Traces: A multilingual series of cultural theory, vol. 4, pp. 5-49.

Bigo, D (2006b): *Security, exception, ban and surveillance.* In: D Lyon (ed.), Theorizing Surveillance. The Panopticon and Beyond. Willan Publishing: Cullompton.

Bigo, D (2002): *Security and immigration: toward a critique of the governmentality of unease.* Alternatives, vol. 27, no. 1, pp. 63-92.

Bodyscanningcrm (2013): *Neopren Wetsuits & Kompressionsbekleidung.* Body Scanning CRM.de, viewed 29 December 2013, http://www.bodyscanningcrm.de/de/textil/neopren-wetsuits-kompressionsbekleidung

Brown, JS; Duguid, P (2000): *The Social Life of Information.* Harvard Business School Press, Boston.

Brown, L (2012): *European Union bans full body airport scanners over safety concerns… so why are they still allowed in the US?* Daily Mail.co.uk, viewed 27 December 2013, http://www.dailymail.co.uk/news/article-2204707/X-ray-technology-Full-body-scanners-banned-Europe-allowed-United-States.html

Burns, B (2013a): *Rapiscan Backscatter Contract Terminated – Units to be Removed.* The TSA Blog.gov, viewed 27 December 2013, http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract.html

Burns, B (2013b): *Body Scanners Resolution Rooms Conduct & Privacy.* The TSA Blog.gov, viewed 30 December 2013, http://blog.tsa.gov/2013/01/body-scanner-resolution-rooms-conduct.html

Burns, B (2013c): *Body Scanner Resolution Rooms Conduct & Privacy.* TSA Blog.gov, viewed 28 December 2013, http://blog.tsa.gov/2013/01/body-scanner-resolution-rooms-conduct.html

Burns, B (2013d): *TSA Week in Review: 30 Firearms Discovered at Security Checkpoints This Week (25 Loaded).* The TSA Blog.gov, viewed 28 December 2013, http://blog.tsa.gov/2013/01/tsa-week-in-review-30-firearms.html

Burns, B (2011a): *Airport Testing of New Advanced Imaging Technology Software Begins Today!* The TSA Blog.gov, viewed 27 December 2013, http://blog.tsa.gov/2011/02/airport-testing-of-new-advanced-imaging.html

Burns, B (2011b): *TSA in the Tabloids.* The TSA Blog.gov, viewed 29 December 2013, http://blog.tsa.gov/2011/10/tsa-in-tabloids.html

Burns, B (2010a): *TSA Purchases Additional Advanced Imaging Technology Units (And a Quick Word on Automated Target Recognition).* The TSA Blog.gov, viewed 27 December 2013, http://blog.tsa.gov/2010/04/tsa-purchases-additional-advanced.html

Burns B (2010b): *Advanced Imaging Technology Automated Target Recognition.* The TSA Blog.gov, viewed 27 December 2013, http://blog.tsa.gov/2010/09/advanced-imaging-technology-automated.html

Burress, C (2004): Clothes-minded moderns eschew Olympic tradition. In ancient Greece, nudity was Games' great equalizer. SFGate.com, viewed 28 December 2013, http://www.sfgate.com/sports/article/BERKELEY-Clothes-minded-moderns-eschew-Olympic-2704765.php

Campbell, D (1998): *Writing Security: United States Foreign Policy and the Politics of Identity.* University of Minnesota Press, Minneapolis.

Caparini, M (2004): Media and the Security Sector: Oversight and Accountability. In: M, Caparini (ed.), Media in Security and Governance. Nomos, Baden-Baden.

Cate, Fred H. (1997): *Privacy in the information age.* Brookings Institution Press, Washington.

Cavoukian, A (2009a): *Whole Body Imaging in airport scanners: Building in privacy by design.* Ipc.on.ca, viewed 28 December 2013, http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf

Cavoukian, A (2009b): *Transformative Technologies deliver both security and privacy: Think positive-zum not zero-sum.* Ipc.on.ca, viewed 28 December 2013, http://www.ipc.on.ca/images/Resources/trans-tech.pdf

CeRI (2013): *The Public Interface Project (Phase I)*. Cornell e-Rulemaking Initivative.org, Viewed 28 December 2013, http://ceri.law.cornell.edu/project-public-int.php

Chan, C (2013): *The TSA Has Finally Removed All of Its Naked Full-Body Scanners.* Gizmodo.com, viewed 29 December 2013, http://gizmodo.com/the-tsa-has-finally-removed-all-of-its-naked-full-body-510797507

Coleman, CL (1993): *The influence of mass media and interpersonal communication on societal and personal risk judgments.* Communication Research, vol. 20, no. 4, pp. 611-628.

Congressional Research Service (2012): *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening.* CRS, Washington.

Cover, R (2003): *The Naked Subject: Nudity, Context and Sexualization in Contemporary Culture.* Body & Society, vol. 9, no. 3, pp. 53-72.

Currah, P; Mulqueen, T (2011): *Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport.* Social Research, vol. 78, no. 2, pp. 557-582.

Curtin, D (2003): *Digital Government in the European Union: Freedom of Information Trumped by "Internal Security".* In: National Security and Open Government. Campbell Public Affairs Institute, Syracuse, New York.

Dandeker, C (1990): *Surveillance, Power and Modernity.* Polity Press, Oxford.
Daston L; Galison P (2007): *Objectivity.* Blackwell, Oxford.

DeMarrais, E; Castillo, LJ; Earle, T (1996): *Ideology, Materialization, and Power Strategies.* Current Anthropology, vol. 37, no. 1, pp. 15-31.

Deutscher Bundestag (2010): *Aktueller Begriff: Körperscanner.* Wissenschaftliche Dienste, Berlin.
Dewey, J (1938): *Logic: The Theory of Inquiry.* In: JA, Boydston (ed.), The later works of John Dewey. Southern Illinois University Press, Carbondale.

Dudgeon, DE; Lacoss, RT (1993): *An overview of automatic target recognition.* The Lincoln Laboratory Journal, vol. 6, no. 1, pp. 3-10.

Dunwoody, S; Peters, HP (1992): *Mass media coverage of technological and environmental risks: A survey of research in the United States and Germany.* Public Understanding of Science, vol. 1, no. 2, pp. 199-230.

Eckermann, L (1997): *Foucault, embodiment and gendered subjectivities. The case of voluntary self-starvation.* In: R, Bunton; A, Peterson (eds.), Foucault, health and medicine. Routledge, New York.

EPIC (2013a): *EPIC v. DHS (Suspension of Body Scanner Program).* EPIC.org, viewed 28 December 2013,
http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html

EPIC (2013b): *About EPIC.* EPIC.org, viewed 28 December 2013,
http://epic.org/epic/about.html

EPIC (2013c): *EPIC Alert.* EPIC.org, viewed 28 December 2013, http://epic.org/alert/

EPIC (2013d): *EPIC in the News.* EPIC.org, viewed 28 December 2013, http://epic.org/news/epic_in_news.html

EPIC (2011): *EPIC v. DHS (Petitioners' Petition for panel rehearing or rehearing en banc and to vacate agency rule).* EPIC.org, viewed 28 December 2013, http://epic.org/privacy/body_scanners/Petition%20for%20Rehearing.pdf

Ewald, F (2002): *The return of Descartes' malicious demon: An outline of a philosophy of precaution.* In: T, Baker; J, Simon (eds.), Embracing risk: The changing culture of insurance and responsibility. University of Chicago Press, Chicago.

Fairclough, N (2001): *Language and Power*. Longman, London.

Farraj, A (2011): *Refugees and the biometric future: The impact of biometrics on refugees and asylum seekers*. Columbia Human Rights Law Review, vol. 43, no. 1, pp. 891-941.

Fish, S (1981): *What is stylistics and why are they saying such terrible things about it?* In: D, Freeman, (ed.), Essays in Modern Stylistics. Methuen, London.

Foucault, M (1975): *Discipline & Punish: The Birth of the Prison.* Vintage Books, New York.

Friedewald, M; Wright, D (eds.): *Two Future Scenarios of Smart Surveillance Applications.* Deliverable 2.1, SAPIENT Project.

Friedman, A (2011): *Towards a Sociology of perception: Sight, sex, and gender.* Cultural Sociology, vol. 5, no. 2, pp. 187-206.

Frimpong, A (2011): *Introduction of full body image scanners at the airports: A delicate balance of protecting privacy and ensuring national security.* Journal of Transportation Security, volume 4, no. 3, pp. 221-229.

Furedi, F.(2007): *The only thing we have to fear is the "culture of fear" itself.* Spiked-Online.com, viewed 29 December 2013, http://www.spiked-online.com/newsite/article/3053

Furedi, F (2002): *Culture of Fear: Risk Taking and the Morality of Low Expectation.* Continuum, London.

Garfinkel, S (2001): *Database Nation:* The Death of Privacy in the 21st Century. O'Reilley, Cambridge.

Gargan, EA (1994): *The Media Business; Reed-Elsevier Building Big Presence in the U.S.* NYT.com, viewed 28 December 2013, http://www.nytimes.com/1994/10/06/business/the-media-business-reed-elsevier-building-big-presence-in-the-us.html?src=pm

Gerety, T (1977): *Redefining Privacy.* Harvard Civil-Rights Liberties Law Review, vol. 12, no. 2, pp. 233-296.

Gill, M (ed.) (2003): *CCTV.* Perpetuity: Leicester.

Gillmor, D (2010): *"Porno-scanners": At last, the public objects.* Salon.com, viewed 11 October 2013, http://www.salon.com/2010/11/15/protesting_strip_search_scans/

Goldman, E (2002): *The Privacy Hoax.* Forbes, viewed 28 December 2013, http://www.forbes.com/forbes/2002/1014/042.html

Gotlieb, CC (1996): *Privacy: A Concept Whose Time Has Come and Gone.* In: D, Lyon; E, Zuriek (eds.), Computers, Surveillance, and Privacy. University of Minnesota Press, Minneapolis.

Grady, J (1996): *The Scope of Visual Sociology.* Visual Sociology, vol. 11, no. 2, pp. 10-24.

Greenberg, J (2005): *This News May Come as a Shock: The Politics and Press Coverage of Electricity Restructuring in Ontario, 1995-2002.* Canadian Journal of Communication, vol. 30, no. 2, pp. 233-258.

Gregoriou, C; Troullinou, P (2012): *Scanning Bodies, Stripping Rights? How do UK Media Discourses Portray Airport Security Measures?* In: C, Gregoriou, (ed.), Constructing Crime. Palgrave MacMillan, New York.

Grint, K; Woolgar, S (1997): *The machine at work: Technology, work, and organization.* Polity, Cambridge.

Groseclose, T; Milyo, J (2004): A Measure of Media Bias. UCLA.edu, viewed 28 December 2013, http://www.sscnet.ucla.edu/polisci/faculty/groseclose/Media.Bias.8.htm

Habermas, J (1997): *Between Facts and Norms.* Polity Press, Cambridge.

Habscheid, S; Thörle, B; Wilton, A (2013): *Sicherheit im öffentlichen Raum: Eine sprach- und kulturvergleichende Diskursanalyse am Beispiel des Körperscanners (2009-2012).* Zeitschrift für angewandte Linguistik, vol. 58, no. 1, pp. 99-132.

Haggerty KD, Ericson, RV (2000): *The surveillant assemblage.* The British Journal of Sociology, vol. 51, no. 4, pp. 605-622.

Hall, R (2009): *Of Ziploc bags and black holes: The aesthetics of transparency in the war on terror.* In: S, Magnet; K, Gates (eds.), The New Media of Surveillance. Routledge, London.

Hall, S (Ed.) (1997): Representation: Cultural representations and signifying practices. Pluto Press, London.

Haraway, D (1988): *Situated Knowledges: The science question in Feminism and the privilege of partial perspective.* Feminist Studies, vol. 14, no. 3, pp. 575-599.

Haußer, K; Mayring, P; Strehmel, P (1982): *Praktische Probleme bei der Inhaltsanalyse offen erhobener Kognitionen, diskutiert am Beispiel der Variablen "Berufsinteresse arbeitloser Lehrer"*. In: HD, Dann; W, Humpert; F, Krause; KC, Tennstädt, (ed.), Analyse und Modifikation subjektiver Theorien von Lehrern. Universität Konstanz, Konstanz.

Henry, G (1995): *Graphing Data.* Sage, Thousand Oaks.

Hier, SP; Greenberg, J; Walby, K; Lett, D (2007): *Media, communication and the establishment of public camera surveillance programs in Canada.* Media Culture Society, vol. 29, no. 5, pp. 727-751.

Hill, K (2013): *TSA Abandons Rapiscan's Nude Body Scanners.* Forbes.com, viewed 29 December 2013, http://www.forbes.com/sites/kashmirhill/2013/01/18/tsa-abandons-rapiscans-nude-body-scanners/

Hoffman, AM; Jengelley, DHA.; Duncan, NT.; Buehler, M; Rees, ML (2010): *How does the business of News influence terrorism coverage? Evidence from the Washington Post and USA Today.* Terrorism and Political Violence, vol. 22, no. 4, pp. 559-580.
Hogan, J (2006): *Letters to the Editor in the "War on Terror": A Cross-National Study.* Mass Communication & Society, vol. 9, no. 1, pp. 63-83.

Hornung, G; Desoi, M; Pocs, M (2010): *Biometric systems in future preventive Scenarios – Legal Issues and Challenges.* In: A, Brömme; C. Busche, Conference of the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG). Springer, Bonn.

Hsieh, HF; Shannon, SE (2005): *Three approaches to qualitative content analysis.* Qualitative Health Research, vol. 15, no. 9, pp. 1277-1288.

Huysmans, J (2004): *Minding Exceptions: Politics of Insecurity and Liberal Democracy.* Contemporary Political Theory, vol. 3, no. 3, pp. 321-341.

Introna, LD; Wood, D (2004): *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems.* Surveillance and Society, vol. 2, no. 2/3, pp. 177-198.

Jackson, R (2005): *Language Power and Politics: Critical Discourse Analysis and the War on Terrorism.* 49th Parallel bham.ac.uk, viewed 29 December 2013, http://www.49thparallel.bham.ac.uk/back/issue15/jackson1.htm

James, C (2000): *Objective knowledge in science: Dialectical objectivity and the history of sonar technology.* Dissertation, University of South Carolina.

Jeffrey, R (2000): *The Unwanted Gaze: The Destruction of Privacy in America.* Random House, New York.

Johnson, J (2010): *One Hundred Naked Citizens: One Hundred Leaked Body Scans.* Gizmodo.com, viewed 27 December 2013, http://gizmodo.com/5690749/these-are-the-first-100-leaked-body-scans

Kaplan, CS (2001): *Kafkaesque? Big Brother? Finding the Right Literary Metaphor for Net Privacy.* NYT.com, viewed 28 December 2013, http://www.nytimes.com/2001/02/02/technology/02CYBERLAW.html

Kellner, D (1990): *Television and the crisis of democracy.* Westview, Boulder.

Kirschenbaum, A (2013): *The cost of airport security: The passenger dilemma.* Journal of Air Transport Management, vol. 30, issue C, pp. 39-45.

Klitou, D (2008): *Backscatter body scanner – a strip search by other means.* Computer Law Security Review, vol. 24, no. 4, pp. 316-325.

Kornblatt, S (2007): *Are Emerging Technologies in Airport Passenger Screening Reasonable under the Fourth Amendment?* Loyola of Los Angeles Law Review, vol. 41, pp. 385-412.

Krippendorff, K (2011): *Discourse and the Materiality of its Artifacts.* In: TR, Kuhn (ed.), Matters of Communication: Political, Cultural, and Technological Challenges to Communication Theorizing. Hampton Press, New York.

Kula, E (2011): *Full-Body Scanners, Live Information and Rights in the Airport: A Theoretical Perspective on Information Circulation.* PhD thesis, Pennsylvania State University.

Lang, K; Engel Lang, G (1994): *The press as prologue: Media coverage of Saddam 1979-1990.* In: WL Bennett; DL Paletz (eds.), Taken by storm: The media, public opinion, and U.S. foreign policy in the Gulf War. University Press of Chicago, Chicago.

LexisNexis (2013): *About LexisNexis.* LexisNexis.com, viewed 28 December 2013, http://www.lexisnexis.com/en-us/about-us/about-us.page

Lextutor (2013): Concordancers. Lextutor.ca, viewed 28 December 2013, http://www.lextutor.ca/concordancers/

Lodato, TJ (2010): *Naked Sight for naked sites: The production of aesthetic Mechanical Objectivity by Advanced Imaging Technology.* PhD paper, Georgia Institute of Technology.

Lynch, M; Woolgar, S (eds.) (1990): *Representation in scientific practice.* MIT Press, Cambridge.

Lyon, D (2007): *Surveillance Studies: An Overview.* Polity Press, Malden.

Lyon, D (2006): *Theorizing Surveillance: The panopticon and beyond.* Willan Publishing, Cullompton.

Lyon, D (2003): *Airports as Data Filters: converging Surveillance Systems after September 11th.* Journal of Information, Communication and Ethics in Society, vol. 1, no. 1, pp. 13-20.

Lyon, D (ed.) (2002): *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* Routledge, London and New York.

Lyon, D (2001): *Surveillance Society: Monitoring everyday Life.* Open University Press, Buckingham.

Magnet, S; Rodgers, T (2012): *Stripping for the State. Whole body imaging technologies and the surveillance of othered bodies.* Feminist Media Studies, vol. 12, no. 1, pp. 101-118.

Manning, PK (2002): *Security in High Modernity: Corrupting Illusions.* Northeastern University, Boston.

Martin, R (2001): The Future of Canadian Security and Defence Policy. Public Opinion and Media Dimensions. CSS Research Paper, Toronto.

Marx, GT (1988): *Undercover: Police Surveillance in America.* University of California Press, Berkeley.

Mayring, P (2010): *Qualitative Inhaltsanalyse. Grundlagen und Techniken.* Beltz Verlag: Weinheim.

McCahill, M (2002): *The Surveillance Web: The Rise of CCTV in an English city.* Willan, Cullompton.

McCartney, J (1997): USA Today Grows Up. American Journalism Review.org, viewed 28 December 2013, http://ajr.org/article.asp?id=878

McCombs, ME (2004): *Setting the Agenda: The Mass Media and Public Opinion.* Polity Press, Cambridge.
McQuail, D (2005): *Mass communication theory*. Sage, London.

Microsemi (2013): *Screening Solutions. Microsemi Passive Millimeter Wave (MMV) Screening Solutions.* Microsemi.com, viewed 28 December 2013, http://www.microsemi.com/products/screening-solutions/

Miller, S (2012): *For Future Reference, a Pioneer in Online Reading.* WSJ.com, viewed 28 December 2013, http://online.wsj.com/news/articles/SB10001424052970203721704577157211501855648

Mironenko, O (2011): *Body scanners versus privacy and data protection.* Computer Law & Security Review, vol. 27, no. 2, pp. 232-244.

Monahan, T (2010): *Surveillance in the Time of Insecurity.* Rutgers University, New Brunswick.

Murakami Wood, D (ed.); Ball, K; Lyon, D; Norris, C; Raab, C (2006): *A report on the Surveillance Society.* Information Commissioner's Office (ICO), Wilmslow.

Nagenborg, M (2011): *Körperscanner.* In: M, Maring (ed.), Fallstudien zur Ethik in Wissenschaft, Wirtschaft, Technik und Gesellschaft. KIT Scientific Publishing, Karlsruhe.
Neuman, WR; Just, MR; Crigler AN (1992): *Common Knowledge.* University of Chicago Press, Chicago.

Nissenbaum, H (2004): *Privacy as Contextual Integrity.* Washington Law Review, vol. 79, no. 119, pp. 144-145.

Office of the Information and Privacy Commissioner of Ontario (1995): *Privacy-Enhancing Technologies: The path to anonymity (Volume I).* OOTIAPCOO, Toronto.

Oram, A (2010): *Current Activities at the Electronic Privacy Information Center*. Oreily.com, viewed 28 December 2013, http://radar.oreilly.com/2010/03/current-activities-at-the-elec.html

Orouji, T; Hosseini, PSM; Jafarizadeh, M; Khosravi HR; Rais, MH (2011): *Doses to the scanned individual and the operator from an X-Ray body scanner system.* Radiation Protection Dosimetry, vol. 147, no. 1-2, pp. 227-229.

Oudshoorn N (2003): The Male Pill: A Biography of a Technology in the Making. Duke Universtity Press, Durham.

Oxford Dictionaries (2013a): *Definition of anomaly in English.* Oxford Dictionaries.com, viewed 27 December 2013, http://oxforddictionaries.com/definition/english/anomaly?q=anomaly

Oxford Dictionaries (2013b): Definition of biometry in English. Oxford Dictionaries.com, viewed 27 December 2013, http://www.oxforddictionaries.com/definition/american_english/biometry

Oxford Dictionaries (2013c): Definition of avatar in English. Oxford Dictionaries.com, viewed 27 October 2013, http://www.oxforddictionaries.com/definition/english/avatar

Page, B (1996): *Who deliberates: Mass media in modern democracy.* University of Chicago Press, Chicago.

Patton, MQ (2002): *Qualitative Research and Evaluation Methods.* Sage, Thousand Oaks.
Pennings, JM; Woiceshyn, J (1987): *A Typology of Organizational Control and its Metaphors*. Research in the Sociology of Organizations, vol. 5, pp. 73-104.

Phillips, N; Hardy C (2002): *Qualitative Research Methods.* Sage, Thousand Oaks.

Pugliese, J (2010): *Biometrics: Bodies, Technologies, Biopolitics.* Routledge, New York.

Rapiscan Systems (2013): *A Security screening leader. A partner you can trust.* Rapiscan Systems.com, viewed 25. September 2013, http://www.rapiscansystems.com/en/company/our_company

Regulations.gov (2013a): *Frequently Asked Questions.* Regulations.gov, viewed 28 December 2013, http://www.regulations.gov/#!faqs

Regulations.gov (2013b): *NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication).* Regulations.gov, viewed 28 December 2013, http://www.regulations.gov/#!docketDetail;D=TSA-2013-0004

Reiman HJ (1976): *Privacy, Intimacy, and Personhood.* Philosophy & Public Affairs, vol. 6, no. 1, pp. 26-44.

Ritsert, J (1972): *Inhaltsanalyse und Ideologiekritik. Ein Versuch über kritische Sozialforschung.* Athenäum, Frankfurt am Main.

Roberts, A (2006): *The Changing Faces of Terrorism.* BBC.co.uk, viewed 27 December 2013, http://www.bbc.co.uk/history/recent/sept_11/changing_faces_03.shtml

Robins, K; Webster F (1989): *The Technical Fix: Education, Computers and Industry.* MacMillan, Basingstoke.

Robinson, JP (1972): *Mass communication and information diffusion.* In: GF, Kline; PJ, Tichenor (Eds.), Current perspectives in mass communication research. Sage, Beverly Hills & London.

Roline, AC; Skalberg, RK. (1998): *Lake v. Wal-Mart: The law of privacy revealed.* ALSB Journal of Employment and Labor Law, vol. 10, pp. 77-83.

Salter, MB (ed.) (2008): *Politics at the airport.* University of Minnesota Press, Minneapolis.

Sanders, J; Cantor, JR (2012): *Joint written Testimony before the United States House of Representatives Committee on Homeland Security Subcommittee on Transportation Security.* TSA.gov, viewed 29 December 2013,

http://www.tsa.gov/sites/default/files/publications/pdf/testimony/tsa-dhs_joint_testimony-11-15-12-ait_concerns-final.pdf

Scheufele, DA; Tewksbury, D (2007): *Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models*. Journal of Communication, vol. 57, no. 1, pp. 9-20.

Schiebinger, L (1993): *Nature's body: Gender in the making of Modern Science.* Beacon Press, New Brunswick.

Schneier, B (2009): *Is aviation security mostly for show?* CNN.com, viewed 28 December 2013, http://www.cnn.com/2009/OPINION/12/29/schneier.air.travel.security.theater/index.html

Schoeman, F (ed.) (1984): *Privacy: Philosophical dimensions of the literature.* In: Philosophical dimensions of privacy: An anthology. Cambridge University Press, Cambridge.

Schreier, M (2012): *Qualitative Content Analysis in Practice.* Sage Publications, London.

Schudson, M (2002): *What's unusual about covering politics as usual.* In: B, Zelizer; S, Alan (eds), Journalism After September 11. Routledge, London and New York.

Seidenstaat, P (2004): *Terrorism, Airport Security and the Private Sector.* Review of Policy Research, vol. 21, no. 3, pp. 275-291.

Select Committee on Intelligence United States Senate (2010): *Attempted terrorist attack on Northwest Airlines Flight 253.* SCOIUSS, Washington.

Sengupta, S (2003): *Signatures of the Apocalypse.* Metamute.org, viewed 28 December 2013, http://www.metamute.org/editorial/articles/signatures-apocalypse

Silverleib, A; Hunter, M (2010): *A primer on the new airport security procedures.* CNN.com, viewed 27 December 2013, http://edition.cnn.com/2010/TRAVEL/11/23/tsa.procedures.primer/

Solove, DJ (2009): *Understanding Privacy.* Harvard University Press, Cambridge.

Solove, DJ; Rotenberg, M; Schwartz, PM (2006): *Information Privacy Law 31*. Aspen Publishers, New York.

Sparapani, T (2006): *Testimony of Timothy D. Sparapani. ACLU Legislative Counsel, on Secure Flight and Registered Traveler before the U.S. Senate Committee on Commerce, Science and Transportation.* ACLU.org, viewed 28 December 2013, https://www.aclu.org/national-security/testimony-timothy-d-sparapani-aclu-legislative-counsel-secure-flight-and-registere

Stafford, BM (1996): *Good Looking. Essays on the Virtue of Images.* MIT Press, London and Cambridge

Staples, WG (2000): *Everyday Surveillance: Vigilance and Visibility in Postmodern Life.* Rowman & Littlefield Publishers, Lanham.

Steinberg, SG (1995): *Electric Word. No Compromise.* Wired.com, viewed 28 December 2013, http://www.wired.com/wired/archive/3.06/eword.html

Strauss, A; Corbin, J (1996): *Grounded Theory: Grundlagen qualitativer Sozialforschung.* Wilhelm Fink Verlag, München.

Strübing, J (2004): Zur sozialtheoretischen und epistemologischen Fundierung des Verfahrens der empirisch begründeten Theoriebildung. VS Verlag für Sozialwissenschaften, Wiesbaden.

Stuntz ,WJ (2006): Against Privacy and Transparency. Prawfs Blawg.com, viewed 28 December 2013, http://prawfsblawg.blogs.com/prawfsblawg/2006/04/against_privacy.html

Subcommittee on Transportation Security Committee on Homeland Security (2012): Rebuilding TSA into a Smarter, Leaner Organization. A Majority Staff Report. SOTSCOHS, Washington.

Suchman, L (2007): *Human-Machine Reconfigurations. Plans and situated actions.* Cambridge Universtity Press, New York.

Suchman, L; Blomberg, J; Orr, JE; Trigg, R (1999): *Reconstructing Technologies as Social Practice*. American Behavioral Scientist, vol. 43, no. 3, pp. 392-408.

Techterms (2013): *User Interface.* Techterms.com, viewed 29 December 2013, http://www.techterms.com/definition/user_interface

Ter Horst, G (2009): *Netherlands: Amsterdam's Schiphol Airport to use body scanners on all US-bound Flights as extra security measure.* ITN Source.com, viewed 27 December 2013, http://www.itnsource.com/shotlist/RTV/2009/12/31/RTV2574009/?v=0

Terre Blache, M and Durrheim, K (1999): *Social constructionist methods.* In: M, Terre Blache; K Durrheim (eds.), Research in practice. Applied methods for the social sciences. UCT Press, Cape Town.

Thomas, DS; Hobson, H; Hubbard, JC; Forcht, KA (2013): *Technology in Practice: Airport scanning privacy issues.* Issues in Information Systems, vol. 14, no. 1, pp. 47-53.

Thomson, JJ (1984): *The Right to Privacy.* In: D, Schoeman (ed.), Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, Cambridge.

Tirosh, Y; Birnhack, M (2013): *Naked in front of the machine: Does airport scanning violate privacy?* Ohio State Law Journal, vol. 74, no. 10, pp. 1-45.

Tran, M (2009): *Body scanners blocked by US "could have prevented attempted plane attack".* The Guardian.com, viewed 28 December 2013, http://www.theguardian.com/world/2009/dec/30/body-scanners-blocked-us-netherlands

TSA (2013a): *Advanced Imaging Technology (AIT).* TSA.gov, viewed 27 December 2013, http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait

TSA (2013b): *AIT: How it Works. Traveler's Guide.* TSA.gov, viewed 27 December 2013, http://www.tsa.gov/ait-how-it-works

TSA (2013c): *About TSA. Innovation and Technology.* TSA.gov, viewed 27 December 2013, http://www.tsa.gov/about-tsa/innovation-and-technology

TSA (2013d): *About TSA.* TSA.gov, viewed 28 December 2013, http://www.tsa.gov/about-tsa

TSA (2013e): *AIT: Privacy.* TSA.gov, viewed 28 December 2013, http://www.tsa.gov/ait-privacy

TSA (2013f): *Risk-based security Initiatives.* TSA.gov, viewed 29 December 2013, http://www.tsa.gov/traveler-information/risk-based-security-initiatives

TSA Office of Security Technology (2008): Office of Security Technology System Planning and Evaluation. Procurement Specification for Whole Body Imager Devices for Checkpoint Operations, TSAOOST, Arlington.

TSA Press (2013): *Press Room.* TSA.gov, Viewed 28 December 2013, http://www.tsa.gov/press

TSA Press (2011): *TSA takes next steps to further enhance passenger privacy.* TSA.gov, viewed 27 December 2013, http://www.tsa.gov/press/releases/2011/07/20/tsa-takes-next-steps-further-enhance-passenger-privacy

TSA Traveler Information (2013): Screening for Passengers 75 and Older. Risk-Based Security. TSA.gov, viewed 29 December 2013, http://www.tsa.gov/traveler-information/screening-passengers-75-and-older

Turkington, RC (1990): *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy.* Northern Illinois University Law Review, vol. 10, no. 2, pp. 479-520.

U.S. Department of Homeland Security (2011): *Privacy Impact Assessment Update for TSA Advanced Imaging Technology.* USDOHS, Washington.

United States Courts of Appeal (2011): *EPIC et. al. petitioners vs. United States Department of Homeland Security et. al. respondents.* USCOA, Washington.

Universitätsbibliothek Wien (2013): *Datenbanken.* Univie.ac.at, viewed 28 December 2013, http://bibliothek.univie.ac.at/fb-rewi/datenbanken.html

US General Service Administration (2013): *Regulations*. USGSA, Washington.

Valverde, M and Mopas, M (2004): *Insecurity and the dream of targeted Governance*. In: W, Larner; W, Walters, (eds.), Global Governmentality: Governing international spaces. Routledge, London.

van Blarkrom, GW; Borking, JJ; Verhaar, P (2003): *PET.* In: GW, van Blarkrom; JJ Borking; JGE, Olk (eds.), Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents. PISA Consortium, The Hague.

van der Ploeg, I (1999): *Written on the body: Biometrics and identity.* Computers and Society, vol. 29, no. 1, pp. 37-44.

Vorderer, P; Groeben, N (ed.) (1987): *Textanalyse als Kognitionskritik? Möglichkeiten und Grenzen ideologiekritsicher Inhaltsanalyse.* Narr, Tübingen.

Wagner, D; Bell, J (2012): *What Israeli Airport Security Teaches the World.* International Policy Digest.org, viewed 10. November 2013, http://www.internationalpolicydigest.org/2012/06/19/what-israeli-airport-security-teaches-the-world/

Walsh, K (2010): *What is a Pat-Down at the Airport?* USA Today.com, viewed 27 December 2013, http://traveltips.usatoday.com/patdown-airport-101838.html

Walton, K (2010): *TSA Screening for Passengers with Mobility Disabilities.* Disability Blog.com, viewed 27 December 2013, http://usodep.blogs.govdelivery.com/2010/12/21/tsa-screening-for-passengers-with-mobility-disabilities/

Warren, SD; Brandeis, LD (1890): *The Right to Privacy.* Harvard Law Review, vol. 4, no. 5 p. 193-220.

Weber, RP (1990): *Basic Content Analysis.* Sage Publications, Newbury Park.

Weinberg, AM (1966): *Can Technology Replace Social Engineering?* University Chicago Magazine, vol. 59, pp. 6-10.

Whitaker, R (2000): *The End of Privacy. How total surveillance is becoming a reality.* New Press: New York.

Widdowson, HG (1995): *Discourse Analysis – a critical view.* Language and Literature, vol. 4, no. 3, pp. 157-172.

Wiles, R; Prosser, J; Bagnoli, A; Clark, A; Davies, K; Holland, S; Renold, E (2008): *Visual Ethics: Ethical Issues in Visual Research.* ESRC National Centre for Research Methods, Manchester.

Wu, A (2004): *The History of Airport Security.* The Savvy Traveler.org, viewed 28 December 2013, http://savvytraveler.publicradio.org/show/features/2000/20000915/security.shtml

Zeeman, L (2000): 'N Diskoers analise: unieke vroue staan op teen gender dilemmas. Ongepubliseerde D.Cur.-proefskrif. Randse Afrikaanse Universiteit, Johannesburg.

Zerubavel, E (2006): *The Elephant in the Room: Silence and Denial in Everyday Life.* Oxford University Press, New York.

Zhang, Y; Wildemuth, BM (2009): *Qualitative analysis of content.* In: B, Wildemuth (ed.), Applications of Social Research Methods to Questions in Information and Library Science. Libraries Unlimited, Westport.

Zureik, E; Hindle K (2004): *Governance, security and technology: The case of Biometrics.* Studies in Political Economy, vol. 73, no. 1, pp. 113-137.

8. Appendix

8.1. Sample

The data for this master thesis are drawn from the following sample of stakeholder documents (SD) from February 2009 to June 2013. The order of the stakeholder documents is numerical. SD stands for Stakeholder Document

No.	Stakeholder	Title	Author	Date
SD 1	Regulations	TSA body scanners are easily circumvented: http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-4662	Sommer Gentry	2013-06-27
SD 2	TSA	TSA Takes Next Steps to Further Enhance Passenger Privacy 1/3: http://www.tsa.gov/press/releases/2011/07/20/tsa-takes-next-steps-further-enhance-passenger-privacy	N.N.	2011-07-20
SD 3	TSA	TSA Announces Additional Advanced Imaging Technology Deployments at U.S. airports: http://www.tsa.gov/press/releases/2011/12/12/tsa-announces-additional-advanced-imaging-technology-deployments-us	N.N.	2011-12-12
SD 4	TSA	TSA Begins Testing New Advanced Imaging Technology Software 1/2 http://www.tsa.gov/press/releases/2011/02/01/tsa-begins-testing-new-advanced-imaging-technology-software	N.N.	2011-02-01
SD 5	TSA	TSA Announces $44.8 for Additional Advanced Imaging Technology at U.S. Airports: http://www.tsa.gov/press/releases/2011/09/07/tsa-announces-448-million-additional-advanced-imaging-technology-us	N.N.	2011-09-07
SD 6	TSA	TSA Administrator John S. Pistole, Homeland Security Polic Institute, George Washington University. Speeches & Testimony http://www.tsa.gov/press/releases/2011/11/10/tsa-administrator-john-s-pistole-homeland-security-policy-institute-george	John S. Pistole	2011-11-10
SD 7	EPIC	TSA Announces “Stick Figure” Software for Some	N.N.	2011-08-02

		Body Scanners 1/2 http://epic.org/alert/epic_alert_1815.html		
SD 8	Regulations	The Use of Nude Body Scanners: http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-4625	Anonymous (N.N.)	2013-06-27
SD 9	Regulations	Regarding the Naked Body Scanners (NBS), I have several comments: http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-2390	Susan Richart	2013-05-29
SD 10	EPIC	TSA Announces "Stick Figure" Software for Some Body Scanners 2/3 http://epic.org/alert/epic_alert_1815.html	N.N.	2011-08-02
SD 11	New York Times	Stripped of Dignity 1/5 http://www.nytimes.com/2011/04/20/opinion/20dowd.html?_r=0	Maureen Dowd	2011-04-20
SD 12	USA Today	States try to legislate TSA screenings; Several lawmakers seek ways to protect privacy by limiting airport security measures http://usatoday30.usatoday.com/news/nation/2011-05-12-invasive-tsa-pat-down-groping-law_n.htm	Alan Levin	2011-05-13
SD 13	New York Times	Stripped of Dignity 2/5 http://www.nytimes.com/2011/04/20/opinion/20dowd.html?_r=0	Maureen Dowd	2011-04-20
SD 14	USA Today	TSA to avoid pat-down searches for kids; Screeners told to be less invasive http://travel.usatoday.com/flights/story/2011/06/TSA-Screeners-will-try-to-avoid-intrusive-patdowns-of-kids/48752944/1	Gary Stoller	2011-06-23
SD 15	TSA	TSA Takes Next Steps to Further Enhance Passenger Privacy 2/3: http://www.tsa.gov/press/releases/2011/07/20/tsa-takes-next-steps-further-enhance-passenger-privacy	N.N.	2011-07-20
SD 16	Regulations	This comment is in response to TSA's NPRM on AIT. The proposed rule raises a number of concerns: http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-4361	Karl Koscher	2013-06-26
SD 17	TSA	TSA Announces Advanced Imaging Technology Deployments at Additional U.S. Airports 1/2: http://www.tsa.gov/press/releases/2011/11/04/tsa-announces-advanced-imaging-technology-deployments-additional-us	N.N.	2011-11-04
SD 18	TSA	TSA Announces Advanced Imaging Technology	N.N.	2011-10-06

		Deployments at Additional U.S. Airports: http://www.tsa.gov/press/releases/2011/10/06/tsa-announces-advanced-imaging-technology-deployments-us-airports		
SD 19	TSA	TSA Announces Additional Advanced Imaging Technology Deployments at U.S. Airports: http://www.tsa.gov/press/releases/2011/12/12/tsa-announces-additional-advanced-imaging-technology-deployments-us	N.N.	2011-12-12
SD 20	TSA	TSA Announces Additional Advanced Imaging Technology Deployments at U.S. Airports: http://www.tsa.gov/press/releases/2012/01/26/tsa-announces-additional-advanced-imaging-technology-deployments-us	N.N.	2012-01-26
SD 21	USA Today	TSA: Airport body scans more “private”; Critics say new software may not ease fliers’ concerns http://travel.usatoday.com/flights/story/2011/07/TSA-says-its-making-airport-screening-more-private/49540660/1	Gary Stoller	2011-07-21
SD 22	Regulations	I do not use full body scanners because I object to the loss of privacy inherent http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-2876	Anonymous (N.N)	2013-06-04
SD 23	TSA	TSA Announces Advanced Imaging Technology Deployments at Additional U.S. Airports 2/2 http://www.tsa.gov/press/releases/2011/11/04/tsa-announces-advanced-imaging-technology-deployments-additional-us	N.N.	2011-11-04
SD 24	New York Times	Stripped of Dignity 3/5 http://www.nytimes.com/2011/04/20/opinion/20dowd.html?ref=maureendowd	Maureen Dowd	2011-04-20
SD 25	New York Times	Stripped of Dignity 4/5 http://www.nytimes.com/2011/04/20/opinion/20dowd.html?ref=maureendowd	Maureen Dowd	2011-04-20
SD 26	New York Times	Screening Still a Pain at Airports, Fliers say http://www.nytimes.com/2011/11/22/business/airport-screening-is-still-a-pain-fliers-complain.html?pagewanted=all&_r=0		2011-11-22
SD 27	New York Times	Stripped of Dignity 5/5 http://www.nytimes.com/2011/04/20/opinion/20dowd.html?ref=maureendowd	Maureen Dowd	2011-04-20
SD 28	New York	Checkpoint Intelligence 1/2	Susan	2011-02-08

	Times	http://www.nytimes.com/2011/02/08/business/08security.html?n=Top%2fReference%2fTimes%20Topics%2fSubjects%2fT%2fTravel%20and%20Vacations&_r=0	Stellin	
SD 29	New York Times	Checkpoint Intelligence 2/2 http://www.nytimes.com/2011/02/08/business/08security.html?n=Top%2fReference%2fTimes%20Topics%2fSubjects%2fT%2fTravel%20and%20Vacations&_r=0	Susan Stellin	2011-02-08
SD 30	TSA	TSA Takes Next Steps to Further Enhance Passenger Privacy 3/3: http://www.tsa.gov/press/releases/2011/07/20/tsa-takes-next-steps-further-enhance-passenger-privacy	N.N.	2011-07-20
SD 31	New York Times	A Farewell to "Nudity" At Airport Checkpoints http://www.nytimes.com/2013/01/22/business/a-farewell-to-nudity-at-airport-checkpoints.html	Joe Sharkey	2013-01-22
SD 32	Regulations	Dear Sirs: I don't think this is necessary.: http://www.regulations.gov/#!documentDetail;D=TSA-2013-0004-3888	Anonymous (N.N.)	2013-06-19
SD 33	TSA	TSA Begins Testing New Advanced Imaging Technology Software 2/2 http://www.tsa.gov/press/releases/2011/02/01/tsa-begins-testing-new-advanced-imaging-technology-software	N.N.	2011-02-01
SD 34	New York Times	Airlines' Holiday Tidings http://www.nytimes.com/2011/10/30/travel/an-update-on-holiday-air-travel.html	Michelle Higgins	2011-10-30
SD 35	EPIC	TSA Announces 'Stick Figure' Software for Some Body Scanners 3/3 http://epic.org/alert/epic_alert_1815.html	N.N.	2011-08-02
SD 36	USA Today	Full-body scans get trial makeover; TSA unveils 'generic' imagery http://usatoday30.usatoday.com/printedition/news/20110202/bodyscans02_st.art.htm	Roger Yu	2011-02-02

8.2. List of figures

8.3. Abstract

Advanced Imaging Technology (AIT) represents a screening method that displaces the use of metal detectors as a standard for passenger controls at airports. The scanners emit electromagnetic waves that bounce off the body surface and create a detailed picture of the skin surface of a passenger. While in test use since 2007, AIT saw a boost in December 2009 when Umar Farouk Abdulmutallab bypassed security controls on Northwest Airlines Flight 253 and managed to smuggle plastic explosives on the plane.

While politicians embraced security of the technology as a means against future terrorist attacks, the public heavily criticized the scanners for invading the privacy of individual travellers. In an effort to refute accusations of AIT as “naked scanners”, the Transportation Security Agency (TSA) released an Automated Target Recognition (ATR) software update in 2011. While the update brings several functional alterations to the screening process, ATR is also discursively restored by efforts to regain confidence in the scanners.

From a STS perspective AIT holds particular interest. ATR software independently takes over the detection process that formerly has been realized by a human operator.

While AIT refers to the human body as a means of identification, the scanners also autonomously decide what appears to be a “normal” body and also whose bodies pose a threat to airport security. Using the concept of mechanical objectivity helps to address the core capability of ATR software to make autonomous decisions. Additionally theoretical concepts of Human-Machine-Interaction, and Visual Sociology inform the examination of stakeholder documents on ATR software.

In utilizing a qualitative discourse analysis it is my goal to follow the discursive traces in documents that can be observed through words and patterns of talk. This thesis features US stakeholder documents, among them newspapers articles, official documents by the TSA and the (EPIC) Electronic Privacy Information Center, as well as public commentaries from regulations.gov. It is the aim of this work to depict the multilayered conceptions of how security and privacy are perceived and discursively realized by various stakeholders in the debate on ATR software.

8.4. Zusammenfassung

Advanced Imaging Technology (AIT) ist eine neuartige Sicherheitstechnologie an Flughäfen, welche die in die Jahre gekommenen Metalldetektoren ersetzen soll. Die Scanner geben elektromagnetische Wellen ab, die vom Körper reflektiert werden und dabei die exakte Darstellung der Körperoberfläche eines Menschen ermöglichen. Obwohl die Technologie bereits seit 2007 an Flughäfen getestet wird, erfuhr AIT erst im Dezember 2009 größere Verbreitung. Damals gelang es Umar Farouk Abdulmutallab Plastiksprengstoff vorbei an Metalldetektoren an Board des Northwest Airlines Flug 253 zu schmuggeln; ein Aufschrei nach neuer Sicherheitstechnologie ging durchs Land.

Während führende Politiker die erhöhte Sicherheit der Technologie preisen, gibt es auch viele kritische Stimmen in der Gesellschaft, die Eingriffe in die individuelle Privatsphäre des Menschen befürchten. Als abfällige Bezeichnungen von “Nacktscannern” längst die Runde gemacht haben, versprach die TSA (Transportation Security Agency) 2011 Besserung durch ein Software Update namens ATR (Automated Target Recognition), mit dem Ziel Privatsphäre-Bedenken zu zerstreuen. ATR Software brachte aber nicht nur funktionelle Änderungen für die Scanner, auch diskursive Veränderungen fanden mit der Vorstellung der Software ihren Weg in die Gesellschaft. Einige dieser diskursiven Veränderungen zielen darauf ab, das verlorene Vertrauen in die Technologie wiederherzustellen.

Aus Sicht der STS weckt AIT besonderes Interesse. Die Scanner bedienen sich des menschlichen Körpers als Mittel zur Identifikation und entscheiden – unabhängig von menschlichem Einfluss – welche Körper einer „Norm“ entsprechen und welche Vorstellungen davon abweichen und somit eine Gefahr für die Sicherheit an Flughäfen darstellen. Das Konzept der „Mechanischen Objektivität“ bietet die Basis um die autarke Erfassung von Gefahrenquellen durch die Scanner kritisch zu hinterfragen. Weiters bietet ATR viele Anreize, die hier theoretisch in Anlehnung an Konzepte der Mensch-Maschine-Interaktion und der Visuellen Soziologie im Zuge der Untersuchung von Dokumenten verfolgt werden.

Mittels einer qualitativen Diskursanalyse versuche ich den sprachlichen Spuren in den Dokumenten zu folgen. Die vorliegende Thesis beschäftigt sich mit Dokumenten von Interessensvertretern in den USA. Neben Printmedien finden sich hier auch offizielle Dokumente der TSA und EPIC (Electronic Privacy Information Center), sowie Kommentare von amerikanischen Bürgern auf regulations.gov. Es ist Ziel dieser Masterthesis die vielschichtigen Vorstellungen von Sicherheit und Privatsphäre in Bezug auf ATR Software

anzuführen und dabei neben der Wahrnehmung dieser Konzepte auch die diskursiven Taktiken der Interessensvertreter aufzuspüren und kritisch zu hinterfragen.

8.5. Curriculum vitae

Education

MA Science-Technology-Society (STS)

2010-2013 (in progress) / University of Vienna, Department of Sociology

Erasmus semester abroad

2011-2012 / Maastricht University, Faculty of Arts and Social Sciences

Bakk. Publizistik- und Kommunikationswissenschaften (Communication Studies)

2006-2010 / University of Vienna, Department of Communication

BA Politikwissenschaften (Political Sciences)

2006-2010 / University of Vienna, Department of Political Science

Work Experience (excerpt)

Freelance Journalist, The Gap Magazin

2007-2013

Chairman, Kollektiv Denkfabrikat

2007-2013

Blogger, card complete Service Bank AG

2010-2011

Backstage Guide, ORF

2008-2010