Hostile Intent - the Terrorist's Achilles Heel?
Observations on Pre-Crime Surveillance by Means of Thought Recognition.

Ralf Kölbel

Professor of Criminology, Criminal Law and Criminal Procedure, University of Bielefeld

Susanne Selter

Assistant to the aforesaid chair, University of Bielefeld

„You do not know beforehand what good or bad you are capable of; you do not know beforehand what a body or a mind can do."[1]

1. INTRODUCTION

One of the fundamental conditions of human interaction is that we are able to look each other in the face, but cannot look behind it. Since the inner life of other people is inaccessible to us, we depend on assumptions we make about the mind of other people. Therefore, we immanently read faces when interacting with other people and we believe that this is a way to understand what a person thinks and feels and what a person is like. In doing so, we tend to go by (also in everyday life) involuntary emotions, as the "natural spontaneity" of such body signs vouches for their authenticity. Sometimes, this is done consciously and virtually methodically, in particular, when there is a special reason to find out more about someone's consciousness rather than concentrating on this person's words. Psychoanalysis, for instance, offers an example of such systematic "body hermeneutics". Moreover, the institutions of state control use such interpretation methods. In judicial and police interrogations, for example, one has always tried to detect lies by carefully examining treacherous expressions. In this respect, the body serves as reference for the assumption that the spoken word differs from the *memory* of an event.

Although the enforcement of behaviour conformity would obviously be supported ideally if hostile intention could be discovered in the face *before* t*he offence*, in the history of the controlling state it has never been possible to pursue this idea systematically or even to institutionalize it. At present, however, as modern terrorism poses a substantial threat to society, there seems to be a notable change. Nowadays, it is assumed that aggressors (individuals, groups, networks, etc.) could – someplace, sometime and somehow – cause immense damages and that they could try and achieve their aims by predominantly using individuals, who have no police record and with whom the traditional alarm systems fail. For this reason, there's a need to find new ways to identify the inconspicuous terrorist in time. One ideal and most reliable solution would be to detect hostile *intent* on the basis of physical indications. Certainly, today this might strike us as adventurous, or not very serious, but what, if such a control technique was developed all the same and preventive recognition of hostile intention became possible? Within the course of this contribution we are endeavoured to answer this question. In the first step we will show that it is actually too late to discuss the topic as if it were fiction, because said methods are

already virtually being developed (2.). In a second step we will put the outlined development in the context of somewhat broader control trends (3.) in order to finally asses them from a critical point of view (4.).

2. THE INDENTIFICATION OF BAD THOUGHTS

2.1. "SPOT" - interactive intention recognition

A couple of years ago, so called "Behavior Detection Officers" (BDO) started to patrol the terminals of U.S.-American airports. On behalf of the "Transport Security Administration" (TSA)[2] these uniformed observers appear to be conducting routine checks. However, they actually focus their attention on the travellers and their behaviour. If somebody behaves strangely, shows signs of fear, of nervousness, of confusion or avoids eye contact, the BDOs start an apparently harmless conversation in the course of which they systematically interpret the face. The conversation is both pretext and inquiry. A preliminary small talk about ordinary topics, within which the BDOs get acquainted with the traveller's facial and bodily expression, is followed by a strategic questioning in order to test the nonverbal reactions prompted thereby. What the BDOs look for, are involuntary signs that betray a suspicious planning. If a suspicious expression of the face or the body is noted, this leads to a physical check of the traveller and his luggage[3]. Instead of confiscating scissors and lighters, the BDOs pay attention to the criminal impulse - the hostile will - of airline passengers.

Such mind reading attempts have their scientific origin in the psychological research on nonverbal communication. The work of Paul Ekman and Wallace V. Friesen, who investigated how emotions are expressed and how they can be read, is of particular importance to this matter. They proved what Darwin had presumed already in his "The Expressions of the Emotions of Humans and Animals": The patterns of emotional mimic are interpreted more or less correspondently in all societies. Ekman spent years to observe facial movements, through which human feelings become visible, and catalogued these expression that can be seen as signs of emotions by us (at least in principle) in a comprehensive, anatomically based "Facial-Action-Coding-System" (FACS)[4]. Hence FACS offers a standardized method of analyzing the facial mimic for deception cues too. As far as the distinction between lying and truth-telling is concerned, the so called "micro-momentary-facial-expression", or "micro-expression", is especially significant. Ekman described the discovery of such volatile, imperceptible movements that reveal a wrong smile and a put-on facade as follows: "In our studies, we recorded interviews set up in such a way that we knew when a person was lying. Afterwards, we replayed the videotapes over and over in slow motion to identify the expressions and behaviors that distinguish lying from truth-telling. We spent hours identifying the precise moment-to-moment movements of the facial muscles (…) to get comprehensive evidence of the kinds of facial looks that accompany spoken lies."[5]

Micro-expressions are withdrawn from our consciousness and self-control. The face develops an independent existence through them, in tense situations they show even in the disciplined face. Admittedly no concealed thinking or planning is reflected immediately in this manner. Only the feeling accompanying the expression is made transparent[6]. Nevertheless, we cannot control this

part of our involuntary, unconscious facial mimic which occurs for less than five-tenths of a second. This is what lets us look behind the forehead[7].In principle every emotional-non-neutral thought can be read - not in the least the evil, criminal and, above all, the terrorist intention. The BDOs just have to inspect closely enough. Thus the BDOs explore "how intent transitions into a visceral mode of anticipatory experience. This, they suggest, can happen in a number of different ways. For instance, the fear of being caught before the act, or the act itself, is anticipated by a terrorist as a sort of feeling. This anticipatory affect is then felt and subsequently experienced in a way which could be identified and read as something like a qualitative emotion, like fear"[8].

These coherences were implemented, for the first time, at the "Ben Gurion"-Airport in Tel Aviv. In good preventive intention, measures to systematically control passengers and to expose their criminal impulse were used there long before 9/11/01[9]. The Israeli experience set the example for the TSA to train about 3000 BDOs in Ekman's mind reading method "Screening Passengers through observational Technique" (SPOT). The technique that could be described as a behavior-pattern recognition system (which rooted exactly in the described notion, that people convey emotions through subconscious gestures and facial expressions) has so far been introduced in 161 U.S. airports[10]. SPOT-training also started in Canada. A first practice test in a real-life context has been announced for this spring[11]. In Europe, SPOT has already been in use since 2006, but only in the realm of the "British Aircraft Authority"[12].

2.2. "FAST" - technical intention recognition

One weak point of SPOT is obvious. The general problem about all kind of surveillance is that human staff is not 100% reliable. BDOs get tired, are diverted, their moods affect their decisions and they are caught up in routines (especially since they almost exclusively meet peaceful people)[13]. Moreover, the personal-intensive use of SPOT-screeners is expensive. The "Homeland Security Advanced Research Project Agency" (HSARPA) therefore prefers an automated recognition of the suspicious micro-expressions and has entrusted a team of scientists with the development of such a technology in 2007[14]. The project's current title is "Future Attribute Screening Technology" (FAST), because the original working title "Project Hostile Intent" seemed much too catchy. Under this label an equipment of virtually surreal character has been developed. The heart of FAST is a computer equipped with a FACS-software. It analyzes an unlimited number of faces which a hidden monitoring camera films while travellers pass an ID-check or queue. Whenever the apparatus notices a face that shows signs of evil intentions, "manual" investigations follow (SPOT-conversations first, police controls afterwards). Additionally, the FACS-computer is extended by a so-called "bio-lidar" (which comprises a group of devices for the recognition of vegetative processes as signs of strain or fear – e.g. a suddenly increased body-temperature, high pulse and blood pressure or heavy respiration)[15]. The instruments work secretly and from a distance. The whole procedure does not take longer than the passport control. Plans already exist to complete the measuring arrangement by a scanner for pupil movements and iris identification, a sensor to analyse messengers in the sweat and to detect the trembling of the body and a magnetic resonance tomography device to uncover compromising neuronal activity[16]. This approach combines a group of different apparatuses (virtually a multi-technology) in order to guarantee the accuracy of identification measurements[17].

The second generation FAST-systems are mobile (FAST M²)[18] and can be positioned wherever more than a handful of people comes together: in railway-stations, on the occasion of sports events, demonstrations, music festivals etc. Furthermore the FAST-System isn't a singular phenomenon. Currently a number of related projects have been set up, that work on miscellaneous (more or less) fully-automated sensor techniques to look (like FAST) behind the forehead and to unveil a malevolent, terrorist intent:

- In Israel a sensor technology (the so called "Suspect Detection System VR-1000") is available that, like a polygraph, is applicable to pre-suspicious persons. Passengers concerned are guided into an open examination- and measuring situation and confronted with questions "that are intended to agitate the guilty respondents and activate certain bodily responses". To this end a variety of stimulating words was collected of which it is believed "only terrorist will respond to". By this means VR-1000 enables an inspection of pre-suspicion in so far as emotional reactions are triggered and become visible "through the measurement of various facial as well as physiological responses" and through "changes in the sonic frequencies of people's voices"[19].
- Israeli security companies strive to optimize the aforementioned concept and fit it for real-time decisions in secret mass use. In the system "WeCu" ("we see you"), which is currently being developed, passengers walk along key stimulators, e.g. pictures of the World Trade Centre Towers or words like "Islamic Jihad" or "Semtex" - that, only unconsciously perceptible, flicker up on utterly harmless departure- and information-boards. Simultaneously, various sensors investigate non-intrusively from the distance (via infrared rays) whether stress indications (body temperature, pulse, skin moisture) occur. Reputed to be more accurate and to measure strain more reliably, these newly tested so-called "smart seats" ("smart carpets", "smart cushions" etc.), are planned to be placed all over waiting- and dispatching areas to record the said physiological data through shoes and clothes[20].
- In their latest project, the experts of the "Paul Ekman Group" commit themselves to the signs of an immediate attack and develop a "Dangerous Demeanor Detector" ("D-Cube") which automatically identifies an expression typical for the pre-assassination attempt phase[21] (for instance the so called "Hinckley-expression", named after John Warnock Hinckley, who tried to kill the former U.S. president Ronald Reagan in March 1981). The software uses video-surveillance-sequences of pre-assassination scenes[22] collected worldwide and enables the recognition of comparably risky situations.
- Finally, the U.S. Department of Defence promotes the development of a small and portable bad-intention-scanner. This mobile device shall record faces like a camera, and, simultaneously, by means of spectral-analysis of psycho-physiological stress-indicators deduce the respective intention in real time[23].

2.3. European correlations

In Europe, there also is a considerable amount of research and development in the field of FAST-related technologies. In 2007, for instance, the European Commission presented the "7th Framework Programme for Security Research"[24] that provides large funds for, amongst others, "ADABTS" ("Automatic Detection of abnormal Behaviour and Threats in crowded Spaces") and for "SAMURAI" ("Suspicious and abnormal Behaviour Monitoring using a Network of Cameras and Sensors for Situation Awareness Enhancement"). These programmes deal with the

development of algorithms and cameras as well as of visual and acoustic sensors to electronically scrutinize and analyse symptoms of danger, indicated by behavioural and situational distinctive features. Some components of these research plans are devoted to perceiving and collecting alarming words, gestures, facial mimics, postures and movements in crowded places. In order to monitor public spaces coordinated devices (film- and sound record by several sensors, locator devices, GPS and RFID-chips) are prepared to localise potential sources of threat and motion analyses[25]. Briefly, any signs and signals human beings use to express themselves shall be observed to classify the overall psychological state of a subject.

As part of the "Information Technology and Media Program under the 6th Framework", the European Union has been supporting the development of computer-based systems for the detection of criminal intent since 2006. Within "HUMABIO"("Human Monitoring and Authentication using Biodynamic Indicators and Behavioral Analysis"), for instance, – a project, financed by the European Commission, – a number of European research institutions work on a combined system for face-, hand pattern-, fingerprint-, voice- and behaviour recognition, that, similar to the mobile FAST-sluice "M²", allows non-invasive, invisible access controls. By measuring brain waves, blood pressure, the respiration rate, etc., the researchers hope to be able to uncover thoughts and plans[26].

Great Britain, where the "Office for Security and Counter-Terrorism" (especially established to pursue the "Science and Technology Counter-Terrorism Strategy" CONTEST)[27], has implemented a programme called "Innovative Science and Technology in Counter-Terrorism" (INSTINCT), promotes the development of a technology that not only detects, but also influences - appeases - a malevolent intent! First and foremost, this project aims to differentiate between someone who is close to committing a crime and someone who is thoroughly peaceful. Moreover, the technology aims at recognizing and processing moods in order to retune hostile persons by controlling and instructing those who surround them. More exact ideas about the technical practicability of these strategies, however, don't seem to exist yet. For that reason, a broader spectrum of scientific subjects (neurology, physiology, psychology, behavioural science, and sociology) is invited to participate[28]. Complementary to this broad research line, pertinent single research projects are invited. Thus the Home Office ordered a "Fear detector" that identifies the assassin by his body odour, more precisely by his fear pheromones[29]. A non-invasive psychological profiling system called "silent talker", which is based on an automated arrangement to interpret the person's frame of mind by measuring, at least in part, involuntary and unintended physiological signs or behavioural variables, has already been introduced in 2006[30].

2.4. The transformation of terror-danger-recognition

Regardless of the extent to which the outlined procedures are still merely a project or already being implemented, they all have one thing in common: They try to avert the danger of terrorism by searching for individuals with terrorist intentions, and, in doing so, use highly personalized search strategies. In the methods of hazard identification, which, in airport handling reach the highest situative concentration by far, FAST and SPOT uniquely embody a transformation from suspicious objects to suspicious *people*. Formerly, controls aimed at identifying objects typically used in all sorts of criminal undertakings: terrorists were determined depending on their means.

Weapons, explosives and components thereof were considered to be the typical attributes of terror. The persons as bearer of individual intentions hardly occured in this monitoring. An unarmed terrorist had nothing to fear, whereas an absolutely innocent person, which happened to be carrying an equivalent of weapons, would have been stopped by the metal detectors and x-ray appliances. With SPOT and FAST the focus of the search strategy has definitively shifted to the "problematical" person. With the new strategies risk identification focuses on individuals as the source of endangerment. The friction between necessary control and preservation of privacy is, however, intensified inevitably with such new control techniques (below 4.3.).

As a result of the outlined processes not only the object of danger recognition but also its *subject* changes. This transformation is marked in particular by the transition from the interactive intention interpretation (SPOT) to the technification typical for FAST. This change exhibits the general characteristics of automated control types: on the one hand, these contrivances compensate evident deficits of the human control potential (in this case our limited abilities to perceive and pay attention), on the other hand, they produce information of "blind objectivity", because the context-bound measurements can only be made clear through human interpretation[31]. Whether the FAST-sensors give an alarm, depends on standardized values, based on physiological indexes for fear and stress and for instincts and drives[32]. The devices react whenever a certain level of symptoms is reached. In contrast, the BDOs act as "hermeneutics", scrutinizing the previously technically sorted out passengers in a SPOT-conversation to get cues for suspicion. Ekman's check list, which contains approximately 35 criteria for hostile intent**,** gives some guidance, but the BDOs still have to rely on their intuition and their interpreting-routines to differ between suspect and non-suspect passengers. Therefore, FAST is an association of the sensorial abilities of the machine and the interpretation skills of the human controller. FAST-tests are so to speak done by "socio-technical-hybrids" - which adds to the explosive nature of this type of control (see 4.3.).

3. THOUGHT RECOGNITION AND CONTROL CULTURES

The outlined methods and projects may strike us as odd considering the seriousness with which an, at first sight, allegedly impossible project like thought reading is carried out. The real problem, however, is quite a different one: what does it reveal about a society when the wish to systematically read what people think not only exists, but is encouraged eagerly by means of the outlined undertakings? To tackle this issue we examine SPOT and FAST and the related concepts in the context of broader trends of state control[33]. Even though the detection of hostile intent is only a small and singular element in this exceptionally wide, multifarious and also contradictory spectrum of modern control instruments, it sets an example for a more comprehensive tendency.

3.1. Classification according to the developments in social control

A formal framework of categories (that was initially developed for other objects by us) allows a useful terminological differentiation and therefore helps to discuss the significance of SPOT and FAST[34]. Within this framework, it is important to distinguish between *control techniques* and

control mechanisms. The individual phenomena of state control (directly perceptible methods and approaches) are called *control techniques*. They are, each in a control modus of its own (i.e. with its own operational logic), laid out for a particular control purpose and hence functionally differentiated[35]. However, control techniques which pursue the same control purposes with the same control modi, can be summarized to groups of structural mutuality (to the said *control mechanisms*)[36]. The variety of control mechanisms, however, necessitates a differentiation of control styles and control regimes. A *control style* is a complex of different control mechanisms or control techniques, as it were an independent control-technical combination. Each control style is characterized by the correspondence of its respective composition and a special control philosophy[37]. As analytic constructions, such distinct control forms do not have empiric correlates. The actually dominating *control structure* rather depends on the *control regime* (a mixture of in fact implemented control techniques) and the accompanying *discourse of control legitimating*. These control-technical and discourse realities are variable and do not only differ from one political system to another, but also change over time. Such shifts of control cultures embed the prevailing *control trends.*

Control trends manifest themselves in a stabilization or withdrawal of control mechanisms or in newly organized control regimes. They often overlap and sometimes they are even contradictory. In this sense, a lot is changing at the moment. For many years, the Western world was influenced by a control culture, in which the regime resembles an interventional control style[38]. Yet *Garland* has called the attention to two newer control trends, namely to a development towards management-wise control techniques and towards an increasing punitivity[39]. In addition, current processes of delegation whereby state control is privatized are often referred to[40]. At the same time, however, a reverse trend is emerging, in that control regimes shift to the control stiles of the "Cooperative Conflict Handling"[41] or extend the concept of "Penal Welfarism"[42]. The claim that a "High Control Society" is currently developing[43], is only partly justified in view of the inhomogeneous and complex control reality. In fact, the High-Control-Formula describes merely one, albeit important part of the present development. The paradigm, widely referred to as "Pre-Crime-Surveillance"[44], also falls into the category of rising control trends and comprises SPOT and FAST as its control mechanisms.

3.2. The emergence of preventive control

"If we wait for threats to fully materialize, we will have waited too long ... we must take the battle to the enemy, disrupt his plans, and confront the worst threats before they emerge."[45] This is the logic of "Pre-Crime-Surveillance" - the logic of pre-emptive preventive tactics and proactive control techniques. Under the label of "Preventive Criminal Offence Fight" or "Proactive Police Action", state authorities search for inquiry impulses and motives irrespective of occasions. In other words: whereas in former control regimes, the authorities used to intervene after threats had emerged, they now actively look for crimes *before* they happen. Their search already begins in phases of clearly less explosive nature and inferior topicality[46]. The state intervenes in situations where there is no impending *danger* (i.e. a serious and imminent threat for a legitimate interest). On the contrary, the intervention takes place either because of a statistical likelihood that damage might occur ("risk"[47]) or just because of a vague expectation of damage ("scenario"). The "*abstract* possibility of the emergence of damage"[48] is sufficient to legitimize the precautionary collection and evaluation of innumerable data (crime-related or in itself irrelevant), and perhaps

even various individualized interferences and the generous gathering of information (e.g. by employing undercover agents). SPOT and FAST also work without the slightest provocation and consequently proceed in the same action logic. “New terrorism remains a high-consequence, low-probability risk“[49]. That’s why the devices are installed to react to perfectly abstract risks based just on the vague expectation that terror attacks might take place somewhere and someday in the future. At the time of the surveillance, none of the travellers is in the least suspicious, not even those, who have criminal intentions. SPOT and FAST are designed to identify initial grounds of suspicion. In this respect, they ideally embody Pre-Crime Surveillance.

To give a very first and preliminary answer to the question of why such a control trend is developing, we have to refer to an interaction process between different social groups. Whenever large parts of the population reflect upon a specific real situation (the de facto existing danger and vulnerability, the in-/efficiency of a previously existing control culture, etc.), the result is a newly constructed reality, influenced by elements of information and moods (habituation, uncertainty, scandalization). All in all, there perception that seems to dominate then sees organized and other serious crimes as a latent but relevant threat. This perception evokes the need to live in a society, free from fear, and produces the strong demand to gain control over all sorts of risk that endanger the well-being within this society. This certainly applies for terrorism, which, above all, is a communication strategy. Primarily modern terrorism – including the enormous devastation, the demonstratively displayed heartlessness of the attacker, the will to die for an ideology, and the constantly upholded threat – conveys the feeling that everyone is constantly endangered[50]. The message “You could be the next“ evokes a feeling of powerlessness and defencelessness, gives the impression that things are getting out of control and is lead to the acceptance of absolutely every control technique that (seemingly) guarantees our security.

Against this background, the preventive controls which promise to protect the safety of social life are accompanied by a wide affinity (within a spectrum that ranges from indifference via acceptance to agreement)[51]. As a response to both the risk and the feeling of being at risk, state institutions boost the control trend of preventive surveillance, which offers structural, juridical and technical innovations as well as the prospect of safety. At first sight, the new methods seem to be much better prepared to fight terror threats than conventional control technologies. If one believes Immanuel Kant, principally, even a fairly reasonable people of devils is special- and general-preventively accessible[52], (Islamic) terrorists however, due to their religious persuasion, are immune to classical sanction threats[53]. Hence preventively applied psychological deterrence proves ineffective. In this respect, terrorists have to be stopped physically in the run-up to their assaults. This again suggests an early diagnosis that starts a long time before the de facto dangerous situation. SPOT and FAST allow an early assessment and furthermore promise to identify the aggressive intention of prospective terrorists who were so to speak invisible – who could not be traced by previous conventional control mechanisms because of their carefully preserved inconspicuousness.

In view of this, SPOT, FAST and other technologies of Pre-Crime Surveillance are functional for society, terror-indicated and for lack of alternatives required. On the other hand, the social perception of threats distorts the actual dangers. This perception, at least isn’t formed autonomously and particularly not unaffected by the media coverage of frightening events. It is, however, vital to understand that said control needs are co-produced by the state[54]. Political protagonists influence the social risk perception along the guidelines of power and influence, of

ideology and economy as well as of the media discourses and the interests of the policing institutions[55]. The fight against terrorism is a benefit and of great utility for all these concerns. The vagueness of the threat in particular contributes to its horrification and makes it easier to establish the acceptance of control in the social discourse[56].

4. CRITICAL EVALUATION

In a preliminary conclusion, SPOT and FAST, as specific control techniques**,** can be seen as typical representatives of the entire Pre-Crime Surveillance control trend and, as such, as building blocks of the new control regimes in the Western world. From a technical point of view, they are an example of a control mechanism according to which a state (because of a potential maximal damage) intervenes in advance, i.e. before any indications for a specific threat are given (see section "K" in the appendix). The fact that this is socially accepted is due to a general, certainly to some extend artificially produced general feeling of threat, fuelled by political interests. Obviously, this doesn't necessarily discredit SPOT, FAST and any related approaches. In this respect, a material evaluation is called for. Below we concentrate on questions of functionality, legitimacy and on the social implications. Reason for scepticism exists on all levels.

4.1. The question of feasibility

First of all, we assume that it is principally possible that the facial mimic and the body language, the voice and gestures give us indications about emotions (particularly with people who try to prevent exactly this by means of self-control). The physical expression, we have to admit, reveals more than an array of deliberately set signals. But even on this basis the intention detection has to cope with serious problems. A system that operates with an inventory of physical indications for lying, criminal intentions and plans for an attack suggests an over-individual, stable connection between expression and emotion. However, it is very unlikely that an individual terror decision produces equal emotions and produces a homogeneous set of bodily expressions – regardless of personality, sex, ethnic group and culture. In reality, already the recognition (let alone the interpretation) of emotions presents difficulties as the intensity of the emotion and their course *vary intersubjectively*[57].

In addition, the interactive intention recognition of SPOT has to overcome further obstacles: Whether the catalogue of dubious body signals the BDOs rely on is valid outside the scientific laboratory and also suitable for selecting passengers which should be subjected to further inspection, isn't obvious at all. Given the usual chaos on airports and the time pressure, it is, moreover, not very likely that the BDOs are capable of reliably monitoring passengers within minutes, whereas experienced experts often need several hours and technical help (slow-motion!) to detect micro-expressions[58]. Despite their integration in the SPOT program, even Ekman and his research colleagues express serious doubts about the feasibility of SPOT in airport settings. They consider it difficult to keep up the concentration and attention that is required for the perception of treacherous, but always only briefly (a fifteenth of a second) appearing micro-expressions under field conditions[59]. Moreover, statistics show that SPOT is not very successful.

Police inspections followed in about 5 % of the more than 100.000 SPOT-conversations BDOs were involved in from January 2006 until April 2008. As a result of the investigations, not a single terror suspect was caught. Instead, only about 700 people were convicted; mainly because of less serious offences (possession of drugs and weapons or infringement of the immigration rights)[60].

The mobile FAST-sluice M², on the other hand, promises to be more successful. In September 2008, a first experiment with 140 test persons showed moderately satisfactory results: 4 out of 5 test persons who had been asked to smuggle a forbidden object through the produced controls and to deny this in a subsequent SPOT-inquiry, could be identified[61]. What does this test in a laboratory say about the use of said method in a real situation, though? In a real situation, the recognition potential of the devices is impeded as, so far, we can only speculate about the pre-crime feelings of a terrorist[62]. What does the assassin feel? Is it fear, compassion or grief? The TSA-Screeners do not answer this question - probably because they aren't quite sure about the criteria either. That's why the danger (i.e. the evil intent) definitely cannot be identified clearly.

As long as travellers are screened on the basis of *unspecific* fears and indications of nervousness, an immense rate of false-positives will be the result. How can we distinguish between typical signs of stress provoked by terrorist intentions or signs of normal stress (e.g. because of a time shortage, fear of flying, pleasant anticipation, farewells or restless children)? Members of generally suspicious nations might show the problematical signs merely because they fear the common hostilities. Body signs can only be interpreted within the immediate context of the current behaviour as an expression of emotions anyway. Moreover, additional technical limitations have to be taken into consideration. If FAST were be able to measure brain activities and to disclose lies[63] or even hostile intentions[64], it is doubted strongly that these intentions could be sorted out in passing[65]. Altogether, even a perfect intention reading technology must fail because of methodological limits.

In the end, success deficits and feasibility limitations are not crucial. If Pre-Crime-Surveillance through SPOT and FAST can be explained alone by the fact that a socially constructed impression of constant threat demands for security improvements, it all depends on the *communicative effects* of the systems. The social relevance of these systems is not a reflection of their real efficiency, but rather depends on the consequences and the extent to which the said systems are a topic in the societal control discourse. At the moment, we can only make assumptions about this. It could be possible that the new control techniques suggest an effective protection measure offered by the state and, as intended, inspire politically functional confidence to calm down the people. It is, however also conceivable and even more probable that the said measures generate more need for security. This is why each protection instrument becomes a part of the risk discourse[66]. By demonstrating its necessity through its existence, it serves the risk perception and the reproduction of insecurity[67]. To paraphrase *Deleuze: "*Risk prevention never stops to start"[68]. Hence, security remains a desired but never attained ideal which constantly generates even more excessive strain. To put it with *Tony Blair*: "What we are desperate to avoid is the situation, where at a later point, people turn around and say: "If you'd only been vigilant as you should have been, we could have averted a terrorist attack."[69]

4.2. The social concomitants

The fact that the actual detection performance SPOT / FAST is marginal and that these contrivances find their expression mainly in the sphere of symbols and communication does not mean that they have no substantial impacts. On the contrary, a number of unintended side-effects does change society. So far, the effects were not particularly beneficial.

- information discrepancy with *misuse potential*: SPOT and FAST produce a myriad of intimate data. Moreover the BDOs set out their observations on date, time, airport, flight number and behavioural oddities in a report. For the purpose of generating risk profiles the TSA stores all the information in a database for a period of 25 years[70]. Such procedures allow a nearly boundless further use of the data. On top of that, nobody can guarantee the information only circuits in the computer networks of the police and the intelligence services.
- effect of *anxiety*: An anxious feeling of being monitored will spread among the travellers as soon as the existence of the undifferentiated intention detection becomes known sufficiently well. Since FAST operates secretly (because the traveller has no notion that his bodily functions and his facial expressions are being monitored) it is even more likely to evoke mistrust. The awareness of being observed (without knowing where, when, to what extent and with which result) easily evokes mistrust and distance as well as shyness and anxiety[71]. Even people who generally accept Pre-Crime Surveillance theoretically may be subject to these feelings as well, when they are directly affected.
- *Net-widening*-impact: As SPOT, FAST and other Pre-Crime Surveillance methods take measures in case of a threat scenario and everybody - law-abiding or not - is checked without exception (which is typical for pre-crime tactics) a huge amount of non-terror-related information is gained (in German legal terminology "Zufallsfunde"). Not for nothing SPOT has so far exclusively spotted less serious offenders (above 4.1.). Against this backdrop a subtle *functional transition* is taking place. The TSA for example underlines the suitability of FAST as a universal method for the monitoring of public space[72]. Some years ago the U.S.-minister of Homeland Security proposed to use intention recognition in criminal proceedings[73]. Finally, in Great Britain the Israeli "voice risk analysis" has recently been tested as a polygraph towards social welfare applicants[74].
- *expansion* tendencies: If, in future, pre-crime detectors work accurately, they will become redundant at the places of their initial use. Terrorists will avoid airports and move on to other, softer targets (like churches, concert halls, production plants etc.). In order to protect these trouble spots, sluices will have to be installed there too. This unavoidable shift has been described in relation to other control techniques[75]. Pre-Crime Surveillance and the war on terrorism will not be exceptions; it's no coincidence that the improvement of mobile FAST devices is as eagerly supported as it is (above 2.2).

4.3. Normative rejections

In addition to these worrying effects a number of questions arise from a normative perspective. It must be questioned whether SPOT and FAST are compatible with the self-esteem of Western cultures and their rule of law. In this respect, it is necessary to highlight once more that, as has been sufficiently proved, there is no freedom without security, but at the same time no security without a certain reduction of freedom[76]. Compared to the recent interdependences between

freedom and security the Pre-Crime Surveillance, however, has undoubtedly led to a shift: it has *lowered* the traditional *thresholds* (danger, suspicion) of the restriction of freedom. The situation, where a passenger is confronted with SPOT and FAST (i.e. when travelling by air) belongs to the neutral everyday performances and in this sense to the most basic exercises of freedom. Although it might certainly be debatable whether the architecture of freedom comes in imbalance from such a shift[77], the described change is clearly of use to the instigators of the presumed dangers: the terrorists. The western society submits itself to a provoked overreaction by leaving behind in a panic its moral standards that are based on the dignity of the Fundamental Rights[78].

All this becomes more obvious, the more precisely the qualities of the intention recognition are reflected and the transition from SPOT to FAST is analysed. At first glance the new control-contrivances might not seem very problematical. They leave no traces on the body and repercussions on feelings and behaviour occur only in the long term. However, the fact that these measures seem to have so mild an effect, is only because they are not felt by the person concerned at the moment they are used (in fact he or she cannot even detect them). But in point of fact they do aim at the personality of each individual passenger in a massive way (above 4.2). Although only the non-intelligible reactions of the body - and in so far depersonalized entities - are registered, *the goal, nevertheless,* is the personal substrate and the place where the personality is formed and where thinking and feeling have their origin! The physiological observations (SPOT) as well as the physiological measurements (FAST) are keys to our utmost individuality and they tend to open the way to *our ego*[79]. And this is even more intensified by the attempt to avoid false positives and to achieve a higher accuracy by combining the devices, because of the thereby increased number of interferences.

It is true that criminal procedure for example knows similar rigorous techniques (e.g. interactive and automated lie detection). This, however, only ever affects a single person. Moreover this person has already been placed under suspicion due to evidence. In contrast to that SPOT and FAST operate before the danger actually occurs and therefore no traveller is left out. Since the familiar identification- and alarm systems fail to catch modern assassins (because there is nothing conspicuous about them at all) the authorities feel forced to interpret the condition of an enormous number of not yet suspicious and never suspicious people. On the level of input (not on the output-level) SPOT and FAST treat everyone in the same way. In that they avoid any "selective discrimination", they are typical exponents of *systematic mass control* and not only qualitatively but also quantitatively excessive. They *combine* - probably in a unique way - the method of thought reading with the screening technology. Each element might be acceptable (if at all) only in itself: the mass screening, provided the consequences for the countless individuals are marginal[80], and the thought reading only as an exception and with the consent of the person concerned. The combination (i.e. the extensive mass spying on thoughts), however, is not tolerable.

5. CONCLUSIONS

Since Pre-Crime-Surveillance fights against crime and terror independent of any concrete indication of offence, it clearly shows an expansive tendency. The logic of Pre-Crime tends to perceive new types of danger with ever changing methods based upon more and more diffuse

signals as early as possible. As far as SPOT and FAST are concerned, this boundlessness is to be grasped with both hands. In the security-paradigm monitoring always tries to provide transparency and to make the invisible visible. The Closed Circuit Television (CCTV) has become the symbol of this logic. Its watchful eye shall help to make the world legible, intelligible and safe. Today however, as the promise of total security turned out to be an empty one, new monitoring techniques even look inside our heads. SPOT and FAST are the warning signals of a completely uninhibited precaution-hubris, which accepts no normative bounds, but only the limitations of the technically feasible. After all, if not even thinking remains absolutely private, which domains for freedom and privacy will be left? Many regard the freedom of the thought as one of the big topics of the 21st century. The fact that various vehement approaches are made to abolish exactly this freedom, proves the urgency of our discussion.

Appendix

control mechanism	**A**	**B**	**C**	**D**	**E**
control goal	settlement	justice	shift of conditions	norm confirmation	stabilization
control mode	habitualized self-control (actor)	-	habitualized self-control (actor)	trust in norm continuity (society)	exclusion of behavioural options (actor)
control technique (examples)	restorative justice	just deserts	disciplining, social therapy, education	demonstration of norm continuity	selective incapacitation, imprisonment

control mechanism	**F**	**G**	**H**	**I**	**K**
control goal	exclusion	deterrence	reduction of opportunities	risk management	risk prevention
control mode	isolation (actor)	situative calculation (actor)	exclusion of behavioural options (actor)	offence handling (society)	danger recognition (society)
control technique	execution, preventive detention, shame sanction	sanction pressure, police presence, video surveillance	gated communities, defensible space, technical security	harm reduction, plea bargaining	data gathering, causeless panoptic control

1 G. Deleuze, ´Ethology: Spinoza and us`, in *Incorporations*, J. Crary, S. K. Winter, eds. (New York 1988) p. 625.

2 The TSA organizationally belongs to the „U.S.-Department of Homeland Security".

3 The SPOT-Screening is describes in: http://www.tsa.gov/press/where_we_stand/training.shtm. (last visited April 26, 2010); L. Herbert, ´Othello Error: Facial Profiling, Privacy, and the Suppression of Dissent`, 79 *Ohio State Journal of Criminal Law* (2008), p. 80 ff.; http://www.time.com/time/nation/article/0,8599,1727625,00.html. (last visited April 26, 2010).

4 P. Ekman, W. Friesen, *Facial Action Coding System: A Technique for the Measurement of Facial Movement*, (Palo Alto 1978); For methods to interpret mimic emotional expressions in general: P. Ekman, *Emotions Revealed: Understanding faces and Feelings* (London 2003); E. L. Rosenberg, ´The Study Of Spontaneous Facial Expressions in Psychology`, in *What the Face reveals: Basic and applied Studies of Spontaneous Expression using the Facial Action Coding System (FACS)*, P. Ekman, E. L. Rosenberg eds. (Oxford 2005) pp. 3, 13.

5 P. Ekman, M. O´Sullivan, M. Frank, ´A few can catch a liar`, 10 *Psychology Science* (1999) pp. 263, 266.

6 The term „thought reading", in so far, is not precisely right; rather a physical feeling-sequence is read and interpreted. P. Root Wolpe, K. R. Foster, D. D. Langleben, ´Emerging Neurotechnologies for Lie-Detection: Promises and Perils`, 5 (2) *American Journal of Bioethics* (2005) pp. 39 - 49, p. 45; S. Schleim, *´Mind reading - Pioneer Work of Brain Research`* (London 2008) p. 22.

7 For the potential of lie detection on the basis of lie-accompanying expressions: P. Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics and Marriage* (New York 2001); A. Vrij, *Detecting lies and deceit, Pitfalls and opportunities* (Chichester 2008); sceptically about the reliability: S. Porter, L. ten Brinke, ´Reading between the lies: Identifying concealed and falsified emotions in universal facial expressions`, 19 *Psychological Science* (2008) pp. 508 - 514.

8 J. Bourke, *Fear: A Cultural History* (London 2005).

9 http://www.nytimes.com/2006/08/17/washington/17screeners.html?. (last visited April 26, 2010); http://www.israel21c.org/technology/us-airport-security-enters-a-new-age-thanks-to-israeli-expertise (last visited April 26, 2010).

10 http://www.tsa.gov/press/happenings/boston_bdo_spot.shtm (last visited April 26, 2010); http://www.tsa.gov/press/speeches/air_cargo_testimony.shtm (last visited April 26, 2010); http://www.tsa.gov/press/where_we_stand/training.shtm. (last visited April 26, 2010).

11 http://www.tc.gc.ca/eng/mediaroom/releases-22010-h002e-5794.htm. (last visited April 26, 2010); http://homelandsecuritynewswire.com/behavioral-observation-comes-canadas-airports. (last visited: April 26, 22010).

12 http://www.timesonline.co.uk/tol/news/uk/article614380.ece. (last visited April 26, 22010); http://www.israel21c.org/technology/us-airport-security-enters-a-new-age-thanks-to-israeli-expertise. (last visited April 26, 2010).

13 For a similar problem with the staff, supervising video monitoring devices: C. Heath, P. Luff, *Technology in Action* (Cambridge 2000) p. 88 ff..

14 Description of the project: www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf. (published Dec. 15, 08).

15 About the method of theses systems in general: Y. Yang, A. Raine, T. Lencz, S. Bihrle, P. Colletti, ´Prefrontal white matter in pathological liars`, 187 *The British Journal of Psychiatry* (2005) pp. 320 - 325.

16 For the methodology of the proof of brain activity through fMRI and EEG: D. J. Heeger, A. C. Huk, W. S. Geisler, D. G. Albrecht, ´Spikes versus BOLD: What does neuroimaging tell us about neuronal activity?` 3 (7) *Nature Neuroscience* (2000) pp. 631 - 633; A. Logothetis, ´What we can do and what we cannot do with fMRI`, 453 *Nature* (2008) pp. 869 - 878.

17 http://www.seattletimes.nwsource.com/html/nationworld/2003893183_tsa200.html. (last visited April 26, 2010).

18 A description of FAST M2 is given in: http://www.dhs.gov/files/programs/gc_1218480185439.shtm. (last visited April 3, 2010); http://www.homelandsecurity.org/StakeholdersMay07/PL4_Dietrich.pdf. (last visited April 26, 2010). For the much simpler counterpart „COGITO 4M", built from standard hardware in India, see http://www.ssbi.in/Home/SDS. (last visited April 26, 2010) and http://www.dhs.gov/xres/programs/gc_1218480185439.shtm. (last visited April 26, 2010).

19 P. Adey, ´Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body`, 27 *Environment and Planning D: Society and Space* (2009) pp. 274 - 295, p. 282; as well as the slightly different description at: J. Florence, R. Friedman, ´Profiles in Terror` 17 (2) *George Mason Law* Review (2009) pp. 423 - 481, p. 433.

20 The first mentioned variant is said to be ready to be produced in series. To this and to the advancements see: http://www.reuters.com/article/idUSL29854328. (last April 26, 2010); http://www.techradar.com/news/world-of-tech/terrorists-caught-by-brain-fingerprinting-491015. (last visited April 26, 2010); http://www.morgenpost.de/web-wissen/article1240307/Sind-die-Gedanken-beim Fliegen-noch-frei.html..

21 http://www.paulekman.com/research/currentprojects/; http://www.dangerousdemeanor.com. (last visited April 26, 2010).

22 For comparable German undertakings: D. Heubrock, N. Immerini, U. Mengeringhausen, P. Palkies, ´Das „auffällige unauffällige Verhalten" des Attentäters vor dem Angriff`, *Kriminalistik* (2009) pp. 81 ff.

23 Project A09-034. See for this: http://www.acq.osd.mil/osbp/sbir/solicitations/sbir092/army092.htm. (last visited April 26, 2010); http://www.ftd.de/politik/international/:neue-ueberwachungskameras-am-flughafen-besser-unschuldig-gucken/522539.html. (last visited April 26, 2010).

24 Description of the 7th Framework Programme: ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf.

25 ftp://ftp.cordis.europa.eu/pub/fp7/security/docs/towards-a-more-secure_en.pdf.

26 http://www.humabio-eu.org. (last visited April 3, 2010); http://phealth2007.med.auth.gr/images/ppt/June21Session2.3/pHealth%20HUMABIO_FINAL.pdf. (last visited April 3, 2010); http://www.newscientist.com/article/dn10963-brain-activity-provides-novel-biometric-key.html. (last visited April 3, 2010). For a first pre-test see http://www.humabio-eu.org/pilot_tests.html. (last visited April 3, 2010)

27 Comprehensively to „The United Kingdom's Strategy for Countering International Terrorism": http://www.tsoshop.co.uk. (last visited April 26, 2010).

28 See the advertisement of INSTINCT: http://security.homeoffice.gov.uk/science-and-technology/innovative-science-tech/ (last visited April 26, 2010) und: http://www.science.mod.uk. (last visited April 3, 2010) as well as supplementing http://www.news.bbc.co.uk/2/hi/uk_news/8201130.stm. (last visited April 26, 2010).

29 http://www.city.ac.uk/news/archive/2009/11_November/091109_3.html. (last visited April 13, 2010).

30 J. Rothwell, Z. Bandar, J. O´Shea, D. McLean ´Silent Talker: A New Computer-Based System for the Analysis of Facial Cues to Deception`, 20 *Applied Cognitive Psychology* (2006) pp. 757 -777, http://www.forensic-centre.com/files/TruthTek.pdf. The system was developed however without specific terror reference.

31 D. Nogalla, *Polizei, avancierte Technik und soziale Kontrolle* (Hamburg 1989) p. 106.

32 In this – and only (!) in this (below 4.3.) – regard FAST follows a trend, Foucault calls „Massifying", a „seizure of power (…), that is directed not at man-as-body but at man-as-species". See: M. Foucault, *Society Must be Defended* (New York 2003) p. 243. See also P. Adey, endnote 4, p. 283.

33 For this: D. Garland, ´The *Culture of Control*` (Chicago 2001); see also: D. Garland,´High Crime Societies and Cultures of Control`, in *Kontrollkulturen.* Beiheft 9 zum *Kriminologischen Journal,* H. Hess, L. Ostermeier, B. Paul eds. (2007) pp. 231 - 249; F. Sack, ´Governing through Crime' in *Sicherheit vor Freiheit?*, Fr.-Ebert-Stiftung eds. (Berlin 2003) pp. 59 - 70; J. Simon, *Governing through Crime* (New York 2007); P. Singelnstein, T. Stolle, *Die Sicherheitsgesellschaft* (Wiesbaden 2008).

34 This pattern is also used for other types of analyses and subjects. Here, it only deals with aspects of state control and does not extend to other facets of the control reality (e.g. effects, effectiveness and their limits).

35 In most cases these control goals do not end in themselves, nor are they the final purpose. They are „intermediate goals" while maintaining the social conformity.

36 To important control mechanisms, that can be determined presently in the states of the West, see the two tables in the appendix.

37 Control styles are models, perfect examples or "Idealtypen" in the sense of Max Weber. Examples: ´Penal Welfarism` (combination of techniques of the mechanisms C - E, G, H); ´Traditional European Principles" (combination of techniques of the mechanism B); ´Expressive Sanctioning` (combination of B, F, G); Management-wise-Pragmatic Conflict Handling` (combination of B - E, G - I) and ´Cooperative Conflict Handling` (combination of A and I).

38 In the organization of our tables (appendix) it was a mixture of the control mechanisms B to E and G to H. A detailed description of this culture of control` is given in: D. Garland, *Punishment and Welfare* (Oxford 1985). Internal differentiations of course existed, since the control regimes differed the sectors (for instance the different approaches towards economic-, violent- and juvenile delinquency).

39 D. Garland (2001, see endnote 33). In our organization to this aspect is a stabilization of the control mechanisms E, F and I. At least as far as the punitive-trend is concerned, the possibility to empirically generalize it is discussed dedicatedly. Exemplary for the German discussion: H. Peters, ´Punitive Turn?`, *Kriminologisches Journal (*2009) pp. 179 - 186.

40 See also B. Forst, P.K. Manning, *The Privatization of Policing* (Washington 1999).

41 I. Aertsen, T. Daems, L. Robert, eds*., The Institutionalization of Restorative Justice in Canada: Effective reform or limited and limiting add-on?* (Portland 2006) pp. 167 - 193; G. Johnstone, D. W. Van Ness, eds., *Handbook of Restorative Justice* (Portland 2006).

42 A revitalization of the treatment of criminal offenders as well as a trend of evidence-based programmes is recognizable throughout the western world now. For relevant british programmes see the latest „*Annual Report"* of the „Correctional Services Accreditation Panel"*:* http://www.justice.gov.uk/publications/docs/correctional-services-report-20080-09.pdf. For the „what works"-attitude see the meta-analytical evaluation given by: M. Lipsey, N. Landenberger, S. Wilson, ´ Effects of Cognitive-Behavioral Programs for Criminal Offenders`, *Campbell Systematic Reviews (*2007).

43 P. Singelnstein, T. Stolle, ´Soziale Kontrolle in High Control Societies`, in *Kontrollkulturen*. Beiheft 9 zum *Kriminologischen Journal,* H. Hess, L. Ostermeier, B. Paul, eds., (2007) pp.108 - 118.

44 In our organization this control trend is a stabilization of control mechanism K.

45 G. W. Bush, *The National Security Strategy of the United States of America*, The White House (Washington 2002).

46 N. Pütter*, Der OK-Komplex* (Münster 1998); L. Zedner*,* ´Pre-crime and post-criminology`, 11 *Theoretical Criminology* (2007) pp. 261 - 281; J. McCulloch, S. Pickering, ´Pre-Crime and Counter-Terrorism`, 49 *British Journal of Criminology* (2009) pp. 628 - 645.

47 For the „risk" in a criminological context S. Krassmann, *Die Kriminalität der Gesellschaft* (Konstanz 2003) pp. 108 ff.; G. Mythen, S. Walklate, ´Criminology and terrorism`, 46 *British Journal of Criminology* (2006) pp. 379 - 398, p. 381.

48 This expression is the translation of the phenomenon into legal terms. See for example: R. Wahl, I. Appel, ´Prävention und Vorsorge` in *Prävention und Vorsorge R*. Wahl, ed., (Bonn 1995) p. 88; O. Lepsius, Risikosteuerung durch

Verwaltungsrecht, 63 *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer* (2004) pp. 264 - 315 p. 271.

49 G. Mythen, M. Walklate, endnote 47 p. 387.

50 On behalf of all: U. Schneckener, *Transnationaler Terrorismus* (Frankfurt/Main 2006).

51 The acceptance of so-called „body-scanners" is in so far significant. See: http://www.focus.de/politik/deutschland/deutschland-grosse-akzeptanz-fuer-nacktscanner_aid_471582.html. (last visited April 26, 2010); https://www.datenschutzzentrum.de/video/umfrage_2004.htm. (last visited April 26, 2010).

52 I. Kant, ´Zum ewigen Frieden`, 2. Chapter, Definitivartikel, 1. Extension, *Werke* in sechs Bänden, W. Weischedel, ed., Band VI (Darmstadt 1964) p. 224. The restrictions, undoubtedly indicated here from an empirical view, shall not have any impact in our context.

53 W. Hoffmann-Riem, Freiheit und Sicherheit im Angesicht terroristischer Anschläge, *Zeitschrift für Rechtspolitik* (2002) pp. 497 - 501, p. 499.

54 See the classical study of K. Beckett, *Making Crime Pay* (New York 1997).

55 This can happen in a really falsifying way („moral panics"), if events or individuals, by making advantage of social stereotypes, purposefully are presented as threat, in order to legitimize restrictive measures. See lately: E. Goode, N. Ben-Yehuda*, Moral Panics. The Social Construction of Deviance* (Weinheim 2009).

56 More detailed to the analysis of this discourse from the point of the governmentality thesis: G. Mythen, S. Walklate, endnote 47, p. 388 ff.

57 See for this for example: M. Heller, V. Haynal, ´Perspectives for Studies of Psychopathology and Psychotherapy, in *What the Face reveals: Basic and applied Studies of Spontaneous Expression using the Facial Action Coding System (FACS*), P. Ekman, E. L. Rosenberg, eds., (Oxford 2005) pp. 507 - 508.

58 A. Vrij, endnote 7, p. 40.

59 P. Ekman, ´How to Spot a Terrorist on the Fly`, *Washington Post* Oct. 29, 2006, at B03, and his colleague Mark Frank: http://www.cossa.org/volume23/Volume%2023Issue7.pdf. (last visited April 26, 2010).

60 http://www.canada.com/calgaryherald/story.html?id=9ab9a6eb-78e1-4a6f-8581-fce2e8c08675&k=37479. (last visited April 26, 2010); http://www.washingtonpost.com/wp-dyn/content/article/2007/09/18/AR2007091801891_2.html. (last visited April 26, 2010).

61 http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html (last visited April 28, 09); http://www.nytimes.com/2009/04/29/us/29surveil.html?_r=2. (last visited April 26, 2010).

62 See C. Honts, M. Hartwig, S. Kleinman, A. Meissner, *Credibility Assessment at Portals, Portals Committee Report* (17.09.09) p. 3; B. M. De Paulo, J. J. Lindsay, B. E. Malone, L. Muhlenbruck, K. Charlton, H. Cooper, ´Cues to deception`, 129 *Psychological Bulletin (*2003) pp. 74 - 118.

63 See for lie detection by using fMRI: D. Langleben, J.W. Loughead, BW. B. Bilker, K. Ruparel, A. R. Childress, S. I. Busch, R. C. Gur, ´Telling Truth From Lie in Individual Subjects With Fast Event-Related fMRI`, 26 *Human Brain Mapping (*2005) pp. 262 - 272. For a first overview: H. Greely, J. Illes, ´Neuroscience-based lie detection: the urgent need for regulation`, 33 I 2 - 3 *Journal for Law and Medicine* (2007) pp. 377 - 431.

64 For experimental findings that could be interpreted in this way see: T. Baumgartner, U. Fischbacher, A. Feierabend, K. Lutz, E. Fehr, ´The Neural Circuitry of a Broken Promise`, 64 I 5 *Neuron (*2009) pp.591 - 770.

65 Vgl. C. Bond, B. M. De Paulo, ´Accuracy of deception judgements`, 10 *Personality and Social Psychology Review* (2006) pp. 214 - 234; Granhag P. A., L. A. Strömwall, *The detection of deception in forensic contexts* (Cambridge 2004). p. 87 ff. The same questions, concerning the practicability of such a method, arose years ago when the NASA presented a project called „Computer-Aided Passenger Pre-Screening (CAPPS)". Objections were raised because it was planned to combine personal information about traveller with data about their brain activity and their pulse, both measured from the distance. (For details about the former debate see: http://www.heise.de/tp/r4/artikel/13/13110/1.html. (last visited April 26, 2010).

66 N. Pütter, *Der OK-Komplex* (Münster 1998) p. 69.

67 Instead of many: S. Quensel, ´Der kulturelle Beitrag der Kriminologie zur hegemonialen Kontrolle`, *Monatsschrift für Kriminologie und Strafrechtsreform* (2008) pp. 355 - 389, p. 369.

68 G. Deleuze, *Negotiations 1972 - 1990 (*Frankfurt am Main 1993) p. 254.

69 Tony Blair, quoted in: F. Desroches, ´Policing in the Post 9/11 Era`, *Research and Evaluation Branch, Royal Canadian Mounted Police* (2005) p. 17.

70 http://www.tsa.gov/press/where_we_stand/training.shtm. (last visited April 26, 2010).

71 For this feature, also characteristic for a variety of monitoring techniques, see lately: BVerfG, 1 BvR 256/08, march 2nd, 2010, paragraph 212, 241; H. H. Kühne, ´Bürgerfreiheit und Verbrecherfreiheit - Der Staat zwischen Leviathan und Nachtwächter`, *Rechtspolitisches Forum*, Heft 21, Institut für Rechtspolitik an der Universität Trier (2004) p. 4.

72 http://www.tsa.gov/what_we_do/layers/bdo/index.shtm. (last visited April 26, 2010). F. ex.: in the lead up to presidential inauguration in Jan. 2005, Wash., D.C., Metro police officers used behavioral profiling techniques to patrol subway stations and identify and question suspicious riders (S. Kehaulani Goo, ´Metro Officers Keep a Keen Eye on Riders: New Behavioral Profiling Techniques, TSA Training Help Target Suspicious Subway Passengers`, Jan. 10, *Washington Post* (2005) p. A06.). Similarly, TSA began deploying „Visible Intermodal Protection and Response teams" („VIPR") in Dec. 2005 along Amtrak's Northeast Corridor and Los Angeles rail lines; ferries in Washington state; and mass transit systems in Atlanta, Philadelphia, and Baltimore (http://www.tsa.gov/press/happenings/vipr_blockisland.shtm. [last visited April 26, 2010]).

73 T. Frank, ´Napolitano Backs Security Tech`, Dec. 29, *USA Today* (2008).

74 J . Florence, R. Friedman, Fn. 19, p. 433.

75 For shifts of criminal activities into unmonitored areas: K. S. Williams, C. Johnstone, ´The politics of selective gaze: Closed Circuit Television and the policing of public space`, 34 *Crime, Law & Social Change* (2000) pp. 183 - 210, p. 197; F. Sack, D. Nogala, M. Lindenberg, *Social control technologies. Aspekte und Konsequenzen des Technikeinsatzes bei Instanzen strafrechtlicher Sozialkontrolle im nationalen und internationalen Kontext* (Hamburg 1997) p. 116 ff..

76 See for instance Z. Bauman, *Community. Seeking Safety in an Insecure World* (Cambridge 2001).

77 An inbalance is affirmed for example by: W. Hoffmann-Riem, ´Freiheit und Sicherheit im Angesicht terroristischer Anschläge`, *Zeitschrift für Rechtspolitik* (2002) pp. 497 - 501, p. 498 ff.

78 See also E. von Bubnoff, ´Terrorismusbekämpfung - eine weltweite Herausforderung`, *Neue Juristische Wochenschrift* (2002) p. 2672 - 2676. For a significant statement of the former German terrorist Ulrike Meinhof see http://www.scribd.com/doc/24588805/Letzte-Texte-von-Ulrike-Meinhof. She saw the first aim of terrorism in the endeavour to push the escalation of the counter-revolution. From her point of view this was eminent to expose the repressive structures of the constitutional state.

79 To this concept of a deindividualizing exploration of body signals, that nevertheless aims to read out the centre of personality: M. Foucault, endnote 32, p. 243.

80 Whether it is at all acceptable to raise individual data from a large quantity of humans (who aren't plausibly connected to the threat scenario) in order to verify a complete abstract danger, is doubtful. At least the German constitutional court demands even for preventing a maximum damage a certain probability of threat-realization, whereas the urgency and concreteness of the danger vary with the degree of the feared damage and the affected civil rights (see BVerfGE 112, p. 284 p. 297; BVerfGE 113, p. 348 p. 386.; BVerfGE 115, p. 320 p. 360 f. and stressed again in BVerfG, 1 BvR 256/08 vom 02.03.2010).