Engaging Science, Technology, and Society

ORIGINAL RESEARCH ARTICLE

Gut Feelings and Algorithms: Searching for Harmful Intentions in Airport Security Processes

SYLVIA KÜHNE
RWTH AACHEN
GERMANY

BETTINA PAUL
UNIVERSITY OF HAMBURG
GERMANY

Abstract

Credibility Assessment, truth verification or lie detection – many terms point to the perpetual endeavour of developing procedures that are supposed to ensure the authenticity of others. This is especially true when the place of action is a vulnerable infrastructural site and the target action is to avert threats. Airports are large architectural filtering systems, in which people and goods are channelled through technological and human screening procedures. But airports also serve as a prominent place for imaginaries of automated control technologies. Although at least in Germany, such technologies are still subject to laboratory work and field trials, they share the notion of searching for *harmful intentions* with current filtering systems. Embedded in the nexus of STS scholarship, critical security and surveillance studies, the article sheds light on the differences and commonalities of human-centred suspicion practices at the airport and its envisioned automated equivalents in the laboratory. Based on insights of focused ethnographic research at German airports and in-depth interviews with researchers, the article presents three empirical case vignettes, highlighting the rationales of human border control, airport security screeners and researchers. Focusing on the role of tacit knowledge for identifying indicators for harmful intentions, the human-centred rationale of *baselining* is put into relation to the so-called *ground truthing* in computational contexts. The field insights suggest that, despite their differences, each mode of thinking and doing relies on conceptualising a so-called phenomenon of harmful intentions as a non-verbal physical display, that manifests itself as an epistemological object as well as a single truth.

Keywords

airport security; automation; harmful intent; baselining; ground truthing

Introduction

Since the aftermath of 11th September 2001 (referred to as 9/11 hereafter), airport security has been characterised by the ambition to identify persons that might pose a threat to aviation. The search for a solution in screening the travellers has fuelled socio-technical imaginations (Jasanoff 2015), like a

To cite this article: Kühne, Sylvia, and Bettina Paul. 2024. "Gut Feelings and Algorithms: Searching for Harmful Intentions in Airport Security Processes." *Engaging Science, Technology, and Society* 10(3): 120–146. https://doi.org/10.17351/ests2023.2337.

To email contact Sylvia Kühne: skuehne@soziologie.rwth-aachen.de.

'Tunnel of Truth' (see Magnuson 2008),[1] through which travellers shall pass seamlessly without stopping, unless the screening systems detect something anomalous on them (weapons) or about them (harmful intentions). US-based projects with these detection targets, such as the 'Automated Virtual Agents for Truth Assessments in Real-time' (AVATAR)[2] (O'Shea et al. 2018; Nunamaker, Burgoon and Giboney 2016), have been mimicked by EU-Horizon 2020-funded research: i.e. 'Iborder Ctrl' was developed as an Automated Deception Detection System (ADDS, O'Shea et al. 2018). As applied research outcomes, the aforementioned prototypes exemplify a tinkering with security technologies and support 'solutionist promises' with security politics (Trauttmansdorff 2022, 145). In spite of these attempts to automate intention detection, the verification of travellers' intentions is still processed by humans at the entry interview and behavioural observations by police border guards and airport security screeners, respectively.

The article explores the human- and machine-centred approaches of the search for harmful intentions. Through tracing the rationales within these approaches, such as baselining and ground truthing, we the authors, aim at discerning the epistemological differences and similarities of this particular form of suspicion work.[3] Situated at the nexus of science and security studies (STS), critical security, and surveillance studies, the article is based on a focused ethnography within the field of airport security and in-depth interviews with researchers of automated intent detection systems.[4]

After outlining the key discussion lines on airport security and the creation of suspicion, we introduce the theoretical lens of our analysis. Drawing upon the differentiations of tacit knowledge as in the work of sociologist of science Harry Collins's (2010), we extend this theoretical lens with the concept of material and symbolic filtering (Cubasch, Engelmann, and Kassung 2021). The latter approach allows for the intermediation of the human suspicion work through sociotechnical devices to be considered. Extending the view from materiality to automation the paper further emphasises the imaginaries within the development process of the detection systems (as coined by O´Grady 2021). Subsequently, we present three vignettes concerning different actors, as well as practices from our field of intent detection to illustrate the empirical findings. This is done after introducing the methodological frame of the fieldwork, which entails the practices of human border control, airport

[1] These ideas have been continuously perpetuated, as in the form of the so-called 'Future Attributed Screening Technology' (FAST) of the US Department for Homeland Security (DHS) (Egbert and Paul 2019).
[2] The AVATAR-Prototype has been tested in Canada and the EU (see Elkins et al. 2014), but is, to our knowledge, the only system that has been transformed into a commercial start-up (Discern Science n.d.).
[3] We use the term *suspicion* as a general (collective) mindset that characterises the anticipatory control culture since 9/11, but not as the legally defined category of police work since our observations targeted a much broader suspicion practice than the legal framework defines (see Pollozek and Passoth 2024, 4, 5).
[4] The article is based on field insights of the research project 'Socio-technical systems of anticipatory truth verification in the field of airport security', conducted by the University of Hamburg and the RWTH Aachen University in 2021-2024. It was funded by the German Research Foundation (DFG) – grant number 442224904.

screeners and researchers of automatised intent detection methodological, as well as practical perspectives on automated airport security. Building upon empirical vignettes in each case, we trace the practice of how criteria that lead to suspicion are created, considering the reciprocal influence of knowledge and materiality. In relating each case to one another, we argue that there is a similarity in each rationale, whereby the idea of a single truth is nourished through the procedural reality that they create. By highlighting the situatedness and contingency within the human rationales – which differs from the predefined machine-centred procedures – we close in pointing to the impact on society at large, as well as the article's contribution for the STS scholarship in the area of airport security processes.

Perspectives on Filtering Threats and Sorting People at the Airport

As contemporary airports are sites of contradictions, being both a highly commercialised and a highly securitised space, the impact of this ambivalence for the practices of airport security has been widely scrutinised by scholars within the nexus of STS, critical security and surveillance studies. Within critical security studies, Mark Salter (2008), engaged with the conflicting prerequisites of accelerating the flow of people, luggage and goods, while at the same time intensifying security controls. This leads to situations where in-state security actors find themselves confronted with the special demands, 'where security presents itself as an economic imperative' (Aas, Gundhus, and Lomell 2009, 13). Ethnographic insights like those by Chiara Bassetti (2017, 2021) exemplify the 'mission ambivalence' of airport security screeners, specifically their public-private role, as a 'dialectic' (2017, 3) of the setting. These double demands are also mirrored in the material infrastructure. Sociologist and STS scholar Jörg Potthast (2016, 141) identifies two types of spaces colliding: 'public spaces of anonymity' conflating with spaces 'that urge for a complete identification, before the security checks, providing persons with bad intentions a perfect hiding place in the anonymous crowd, after the security gate a completely recorded and monitored population'.[5] Therefore, both security gates and border technologies have been looked upon either for *what* (kind of policy) they represent, or for *how* they materialise political rationales (see Trauttmansdorff 2022, 135; also Linhardt 2000, 83–89), something that is becoming evident within the shift to proactive security.

Shifting from a Reactive to Proactive Rationale

As the attacks of 9/11 have been described as revealing the weaknesses of airport security (Potthast 2011, 226), aviation matters have since been placed in a special focus of the new security rationale, whose primary ontological contour has been the reshaping of risk in an anticipatory logic (Amoore

[5] Translation by the authors, as all translations from literature and interviews from German to English are by the authors.

2013, 9). As such it differs fundamentally from traditional procedures that based their crime and security control measures on obtaining information about past events. Since 9/11, this former logic of risk, which was based on a probabilistic rationale, has been replaced by a future knowledge related rationale of 'possibilities' (see ibid.). Within this new logic, technological security developments are fuelled by sociotechnical imaginations (Jasanoff 2015) which promise the management of uncertainty (Degenhardt and Bourne 2020). This promise – as STS scholar Lucy Suchman notes in her work on the revival of AI in the military – is linked to the 'enduring premise of objectivist knowledge' within technological systems (2023, 762).

Central to this kind of anticipation of the future are the elements of nonknowledge and incalculability (see especially Amoore 2013), which International Security Politics scholars Claudia Aradau and Rens van Munster (2007) link to the precautionary principle. They do this in order to grasp how the current rationale 'entails drastic prevention at the catastrophic horizon of the future, as well as generalised and arbitrary surveillance at the limit of knowledge' (see also Bigo and Tsoukala 2008, 2). The *limits of knowledge* imply the anticipation of possible futures by means of technology, and the airport is considered an attractive test site for this kind of new security technology (Bourne, Johnson, and Lisle 2015). But besides being a testing ground itself, the airport's demand for the acceleration of control and sorting procedures inspires applied research in the laboratory as well, and hence the focus of our article.

As this manifold utilisation of technologies has been characterised as being part of a broader security assemblage (see Aradau and Blanke 2015), STS scholarship has indicated a social 'demarcation through biotechnological innovations' (Heinemann and Weiß 2016, 9) and thereby scrutinised the development of behaviour-based biometrics for the creation of suspicion (Sutrop and Laas-Mikko 2012; generally on border devices, Pollozek and Passoth 2024). Its underlying rationales have been carved out by sociologist Didier Bigo and criminologist Anastassia Tsoukala (2008, 2); emphasising that the imperative of free movement is transformed through a 'normalisation of social groups whose behaviours are monitored for their present and their future'. Therefore, a majority of passengers is being normalised or *trusted* while a minority is filtered out and treated with suspicion – processes that have been described as 'social sorting' and characterised as deeply economically driven (Adey 2006, 196; more general Lyon 2008, 29–50).

Generating Suspicion through Humans and Automated Systems

The economic driven pre-filtering through programs like the 'US-Trusted Traveller Programme' is just one of many forms of sorting the general public at the airport. This initiative shares a common feature with the on-site filtering procedures: as their logic follows the search for the abnormal within the travelling crowd. This inquiry, embodied through surveillance technologies, has been characterised not only as a general distrust towards every traveller (Aas, Gundhus, and Lomell 2009), but also as security-related *profiling* (Molotch 2014, 125–27). Hence the term and its practice have been widely disputed because of their affiliation with a bias about ethnicity and nationality, for example (see Adey 2009, 277). While it is a common practice in US and Israeli border checks, the

differentiating of travellers by risk status is still disputed when it comes to standard European procedures (Weydner-Volkmann 2017).

Scholars from surveillance studies that have scrutinised versions of sorting procedures (profiling, biometrical reads etc.), such as Peter Adey (2004, 2009), are calling for a more profound network analysis of how to relate the sorting architecture of humans and of objects. Concerning the human-centred line of practice, Adey (2009) has analysed the Behavioural Screening Programme SPOT[6] for the way it discriminates passengers according to a checklist of cues, which are read as possible indicators for harmful intent, such as a terrorist attack. He carves out the resemblance to traditional lie detection rationales (see also Littlefield 2011), thereby pointing to automated screening systems carrying the same logic when relying on future knowledge about how passengers are expected to behave (Adey 2009, 277).

With the rise of computational methods in airport controls, automatised screenings such as the envisioned behaviour anomaly detection are emphasised as a neutral way of profiling (see Chertoff 2007 in Amoore 2009) and are therefore imagined as eliminating the disputed bias of human-centred suspicion practices. Resulting from the situational embeddedness, bias is seen as a result of humans relying on their intuition and experience (see Ferguson 2017, 54). But this claim for objectivity has been challenged, and the few automated detection concepts that have been tested at airports have been scrutinised extensively among others for their reproduction of biases (Egbert and Paul 2018, 2019; Sánchez-Monedero and Dencik 2020; Jupe and Keatly 2020; Sutrop and Laas-Mikko 2012). Although the vast field of detection approaches currently only exists in the laboratory, this critique concerns them equally. It follows a general questioning of the way computational procedures work when offering security solutions. Claudia Aradau and Tobias Blanke (2015, 7) are encouraging researchers to (a) question how the data that is used for the formation of suspicion is collected, particularly whether this is through big data, and (b) to form computational collaborations with social scientists for this debunking endeavour (see e.g. Glouftsios and Leese 2023). This argument is extended through critical algorithmic studies, which explore the co-constitution of algorithms and society (e.g. Lehr and Ohm 2017; Barocas and Selbst 2016) and consider the invisible knowledge production in the use of algorithms (see Bechmann and Bowker 2019; Gillespie 2014; Jaton 2017, 2021; Amoore 2019). As an example, Florian Jaton examines the logic of algorithm-related data accumulation, preparation, and classification, showing that it is based on 'collective problematization, that includes discussions and compromises among different actors' (2021, 78). Thereby, the naturalisation of the technological approach as an objective procedure is already beginning at the level of developing systems, where detection criteria are transferred into algorithms and machine-learning systems (see Egbert and Paul 2018, 2019; Jaton 2021). At the heart of the debate

[6] For further critique of the 'Screening of Passengers by Observation Techniques' (SPOT) programme of the US Transportation Security Administration (TSA) see Denault et al. (2020).

lies what Christoph Musik and Matthias Zeppelzauer (2018, 4) called the 'difference between the 'algorithmic logic' and the 'editorial logic'', which we translate in our context to meaning, which people are considered risky and which indicators are defined as adequate as questions that are negotiated politically rather than decided on by the technology per se (see Amoore 2013, 164).

Conversely, technologies have a 'political rationality' (Jobard and Linhardt 2008, 85). Devices like e-gates or scanners, airport architecture, aviation security laws, and sociotechnical security practices (like access controls) are all part of a 'sociomaterial assemblage' (Suchman 2007). As Fabian Jobard and Dominique Linhardt (2008, 85) highlight in their comparative study on surveillance controls, 'filtering technology' could be 'understood as a form of political semiology', within an 'economy of suspicion' (ibid., 83).[7] This Taylorisation of suspicion functions in the field as a guarantee for efficiency, neutrality and protection of arbitrariness by the state actors (Linhardt 2000, 103). Hence, Linhardt (ibid., 84) showed in detail how security architecture and technology forces people into action formats. In contrast, Fabia Schäufele (2017) explicitly carved out the profiling inscriptions of security devices (see for the inscriptions of suspicion, Pollozek and Passoth 2024), but equally demonstrated that there is a potential of modifying scripts. Similarly, André Biermannn and Stefan Kaufmann (2021) have shown how ambivalences that arise in the detection process open up scope for action on part of security personnel.

Therefore, taking the contingencies of technical procedures into account, Potthast, Linhardt and Jobard share a view that we would like to contest. They describe machine-centred procedures (which date some years back) as positively attributed in their potential to overcome human fallacies. Linhardt highlights that through the focus of suspicion on a collective level, this counts as objectification. According to him, the suspicion is being objectified, because only the externals of the person are taken into consideration through a predefined frame (2000, 103). Similarly, Potthast raises the question: 'Would not visual search by machines be more democratic as compared to manual search carried out by operators following dubious and maybe racist stereotypes of what constitutes a 'dangerous person?'' (2011, 95).

This is where we embed our study, raising the question of what kind of knowledge generates suspicion, followed by the contestation of the envisioned overcoming of bias through the use of computational procedures. Besides the desiderata of an intensification of STS's engagement with security technologies (Degenhardt and Bourne 2020, 209), we intend to fill the blank space of an inquiry into the parallels of human and computational practices on the subject of intent detection.

[7] This emphasises how ontological politics are practice-based within the negotiation of security technologies (see Schouten 2014).

Outlining the Field

The way we take up suspicion within airport security is two-fold: it is part of police work as well as that of airport security screeners;[8] but it is also subject to fields of research within the realms of applied psychology and computational studies, especially those that are engaged with research on automation intent detection, trying to find 'solutions' for large scale applications (Kleinberg, Arntz, and Verschuere 2019; Honts and Hartwig 2014).[9] It is out of these fields of practice that we drew our three case studies (empirical vignettes) for the article, which proved to be of major relevance for exploring the human- and machine-centred approaches in their search for harmful intentions.

The first case study we chose were the border police (vignette 1), who rely heavily on their expert knowledge, accompanied by data-driven technologies. For border police officers, threat analysis is part of their daily work, without being especially trained in behavioural analysis. The work of the distinct group of behavioural analysts within the police (which is still small in numbers in Germany) is not the subject of our analysis, as it is the everyday and common police practice concerning intent detection that we are interested in. The second case (vignette 2) entails the work of security screeners, that screen passengers and their luggage for prohibited items and other threats to security. While their work is also partially automated, the third empirical case (vignette 3) focusses on the work of researchers that conceptualise automated systems for intent detection.

Even though practices of border control and aviation security are inherently different – in their training, aims, focus and regulation – they share the notion of averting threats by techniques such as observing, interviewing, and screening, which is why we characterise both fields as *airport security work*. Just as the research that anticipates the process of automating the detection of harmful intentions, they follow the aim to differentiate and therefore *filter* passengers and objects according to a risk that is anticipated. In the following, we use the term 'filtering' as a cultural technique which emphasises the relation between the material and symbolic essence; as such it refers to a technique of differentiation which evolves an interplay with the environment (see Cubasch, Engelmann, and Kassung 2021, 3, 5). In this way, we can acknowledge the fact that through the emergence of computational methods, the generation of culture is no longer just a matter of human cognition, but also of machine actions.

The focus of this article is to explore the rationales within the different filtering phenomena that aim to detect harmful intent. We understand a rationale thereby in the governmental sense, as a

[8] In Germany they are named *air security assistants*. In this article we use the term *airport security screeners* which is common in the respective literature. It entails the diverse roles of not just screening, but also acting as 'unpacker' and 'attender' (see Bassetti 2021, 601).

[9] The paper is based on the research project 'Socio-technical systems of anticipatory truth verification in the field of airport security', conducted by the Universität Hamburg and the RWTH Aachen University. It was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – project number 442224904.

mode of thinking and doing which forms the perception and assessment of problems, that can be materialised and internalised in certain practices (see Krasmann 2003, 72–73). The most distinct rationales we like to differentiate are those that base the anticipated normalcy regarding the behaviour that is expected in a given context. For both cases of the human-centred filtering process, we identified the rationale *baselining* which we will relate to the logics of the information filtering process from the laboratory that functions on the basis of a (for the STS realms) still rather unfamiliar computational phenomenon of *ground truthing*. A baseline in the respective police psychology literature is predicated as representing 'a level for assessing behaviour', which means for the large-scale context the collective base, which 'forms the 'normal state' for the respective situational context' (Krüger 2019, 193). In contrast, the research is characterised by rationales driven by the perception of a norm and its deviations, which is termed *ground truthing*. The term *ground truth* was originally used in remote sensing science and in geography, where humans are verifying pictures or digitised information about a landmark taken from the air. Today, *ground truth* has become a standard term in computational contexts, where it refers to problems of scaling, in other words transferring reality into technical realms (Gil-Fournier and Parikka 2021). Overall, we can say that the term *ground truthing* describes a practice whereby an anticipated truth is constituted within computational filtering processes (Musik 2016).

In each of the chosen fields, the filtering rationales are entangled in a specific job-related world of thought concerning their social environment. One facet they all share is that they do not explicate the base of the indicators for their filtering of *harmful intention*. The human baseliner who listens to a gut feeling and the machine-based procedure which develops into a black box both rely on a form of tacit knowledge (Collins 2010), which is the common ground on which we will compare them. Collins's (ibid., 1) reflection on tacit knowledge refers to 'knowledge that is not explicated', but as he points out, 'is not' does not mean 'cannot' (ibid., 4, 88–91), and it is this inability to explicate knowledge that is at the base of the detection of intent that we will scrutinise. The relevance of Collins's work becomes apparent when the actors of the suspicion practice are convinced of their knowledge as a kind of somatic and collective of tacit knowledge. This is influenced by what he terms 'collective tacit knowledge', which is inherently located in 'social collectivity' (2007, 257).

When Collins (2010, 123) emphasises 'the kind of tacit knowledge that can only be acquired through social embedding in society', he underlines the inability of machines to adapt to different social settings and their lack of ability to improvise. Both of these factors would hinder the transferral of tacit knowledge to machines. Although this is a plausible argument, Collins neglects other ways of tacit knowledge reaching technological systems – which, for the purposes of this study, we consider to be analogous to *machines*. We argue that, contrary to Collins's reasoning, automated knowledge

itself appears to be necessarily implicit, as it is materialised knowledge.[10] Furthermore, the human-centred filtering practices are supported by architectural and technological filters. These have been delegated to act on suspicion, since the human 'sense of normality' has been inscribed to them (Jobard and Linhardt 2008, 84). Respectively, we take up the concept of human improvisation to illustrate its difference in rationale by comparing it to composition. We borrow this juxtaposition from the field of jazz (Kurt 2008, 36), as the difference of improvisation and composition lies in their relation to time: while the Latin word *improvisus* already implies a meaning of an unforeseeable future, composition is based on decisions made in the past (ibid., 12). Thus, we divide filter techniques into 'composing' filtering versus 'improvising' filtering.

When we look upon automated systems in our field, we target the conceptualisation of detection systems within the laboratory. For this our lens has been coined by Nathanial O'Grady's (2021, 233) perception which goes beyond seeing automation as just 'a set of computational processes integrated into digital technologies'. Instead, he emphasises its relational feature and fosters understanding that does not just consent to the common notion of automation as the depowering of humans, but instead focuses on the question of which imaginaries and expectations in the development of a system are connected to the situative practice in which they are prototyped. For us this means to capture the imaginations of how intent is showing and how the technical systems are supposed to target that. Since they are still devices in the laboratory, this poses the methodological endeavour to capture facets of something that is not even realised yet. We argue though that the pure tinkering[11] with the idea to detect intentions has a reality-constituting effect in itself, just as Mike Bourne and colleagues (2015) show in their field study on the development of a security device.

Since we understand rationales as modes of thinking and doing, the different methodological access for each field turned out to be a fitting way to get a glimpse of each field's rationales in their filtering to detect intent. Therefore, the chosen filtering approaches are suitable for a comparative analysis. Like Potthast's study (2011) on airport access controls shows, it is worthwhile to differentiate between modes of control. He reaffirmed Jobard and Linhardt's (2008) earlier study, in which they compared surveillance modes of airports and no-go areas of a housing project. Similarly, we aim to relate different fields to one another, as they have a shared goal of succeeding in intent detection.

The research was conducted along the lines of the focused ethnographic approach as outlined by Hubert Knoblauch (2001), which focuses on the background knowledge of a field section (ibid., 137). This kind of short term, intensive ethnography requires a familiarity with the field so as to decide

[10] Collins has been criticised for his strong focus on social factors when reflecting on the limits of machines (see Gulick 2023). However, to engage in this discourse is beyond the scope of this paper.
[11] The way we refer to the term 'tinkering' is in the sense of Karin Knorr (1979, 371), who points to the research pragmatic to search for solutions instead of gaining knowledge during research.

on a focus. We gained our ability to focus on field experience from a prior project on lie detection ("From Polygraph to Brain Scan", 2017-2020).[12] For the argument of this paper, we draw on 17 focused observational accounts that we conducted stemming from fieldwork with a duration from a half-day to one-to-two weeks, distributed between three airports and one laboratory in Germany. Furthermore, we draw on 105 ethnographic conversations (with 110 persons and 37 audio-recorded in-depth interviews (with 42 different persons).

Just in line with the way Potthast (2011, 91) reflects on the difficulties of conducting research in the field of airport security (see quite similar to Molotch 2014, 4–6), we were only allowed in the field for a short amount of time, taking field notes instead of tape recordings, which supported the approach of focused ethnography. The access we gained was through snowball sampling and contacts from a former project, as well as directly approaching the field. The in-depth interviews with the scientific field partly had follow-up interviews, which allowed us to deepen the reflections from the field observations.

The collected material was analysed according to the principles of an abductive analysis (Tavory and Timmermans 2014) and coded as analytical themes regarding the concept of the detection procedure, as well as the ontology of intent and automation. Abduction in this sense aims at 'developing speculative theories within a systematic analysis of variation across a study' (ibid., 131). Key to this procedure is the iterative analytical process of relating the material to a diverse corpus of theoretical literature, hereby working on recognising empirical surprises (ibid., 125).

Practising and Conceptualising *Intent Detection*

The new anticipatory security rationales have also been influential in the deception research field, which has classically focused on finding methods to scrutinise individual accounts. Turning to finding applications for large scale operations, such as airports, deception detection technologies emerge with new aspirations for their intentions. One of these is the focus on so-called *false* (as equivalent to deceptive) *intentions* instead of focusing on accounts of one's past actions (see Vrij et al. 2011; Granhag and Giolla 2014; Honts and Hartwig 2014; Kleinberg, Arntz, and Verschuere 2019).

On an epistemological level, the focus on verifying the credibility of intentions can be traced back to key psychological research[13] that presupposes intention as a mental state. This state is accompanied by planning moments, which are the object of detection criteria when it comes to verbal- and content-directed detection methods (Granhag and Giolla 2014, 195). This points to a crucial distinction in the deception research field. It can roughly be divided along an epistemological gap between cognitive theories, rather than theories of emotion- (or arousal-) oriented assumptions for cues of false intentions (see Kleinberg, Arntz, and Verschuere 2019; Vrij, Hartwig, and Granhag

[12] Funded by the German Research Foundation (DFG) – grant number 320725678.

[13] For a review on detection of intention approaches, see Feijoo-Fernández, Carmen, and Halty (2018).

2019). Researchers that are dedicated to cognitive explanations for cues of deception look at the amount of content-based verifiable details (Jupe et al. 2017; see also Verschuere et al. 2023). Emotional- or arousal-based approaches on the contrary are based on the assumptions that nonverbal cues of intention show in the behaviour of people when they are heavily engaged emotionally (i.e. through guilt or fear), and have an additional cognitive load, or try to control their behaviour (for an overview, see Vrij 2008, 37–89).

Even though within deception research it is generally considered that '[t]here are no nonverbal behaviours that are indicative of deception' (Denault et al. 2020, 1), the tinkering with automated approaches of measuring non-verbal behavioural cues continues. The popularity of cues like movement patterns or micro expressions in computational approaches can be traced back to the demand of easy and fast methods 'to address the sheer volume of veracity judgments to be made' (Granhag and Giolla 2014, 198). This stands in sharp contrast to the collectively voiced concerns from the psychological field that these approaches lack theoretical soundness and empirical evidence (Denault et al. 2020; Vrij, Hartwig, and Granhag 2019).

In the actual suspicion work at the airport, police and security screeners rely on given applicable knowledge from their training, which means that they cannot wait for basic research to find helpful answers. This opens the opportunity for providers of quick solutions to step in (see Denault et al. 2020). Meanwhile the human-centred focus of behavioural cues in the form of 'behavioural detection' is on the rise within the field of European airport security.[14] As it is still a heterogeneous field of application, the basic thoughts of observing deviations to an anticipated normalcy relying on behavioural cues is common within daily routines of airport screeners and border police.[15] Their professional background differs sharply, since the years of training (and studying) to become a police officer does not compare to the rather short on-the-job training of a security screener. Nevertheless, there are similarities when it comes to what kind of knowledge has to be applied within the field. Both professions are trained in some form of interviewing and observing behaviour to anticipate threats, combining content-related, verbal and non-verbal cues within their interactive practice.

Border Police: '*Something Isn't Right*'

A large part of the border police work (where we accompanied them) takes place in a small control box, crowded with desks and chairs for the border guards, computer screens and some verification

[14] In Europe, several countries (including the UK, Switzerland, Spain and Germany) have come up with their own versions of a behavioural detection respectively analysis (for an oversight from a police perspective, see Feijoo-Fernández et al. 2023).

[15] As pointed out before, general police work has to be differentiated from the special behavioural analysis for which officers are specifically trained (see Krüger 2019). So far they are not very common within Germany.

devices like the document scanner. During the entry interviews the border guards run the traveller's data through various databases, which sometimes leads to an indication of doubting a traveller's intentions:

> The travellers come to the counter and present their passport, sometimes a residence permit. . . . The officer places the passport in the document scanner to her right and looks at the screen on which the chip image and the visible passport photo are shown. The program *complains* about parts of the scanned passport, which the officer must look at and decide for herself whether she also sees cause for complaint. By checking the databases, she sees a list of red hits that list various documents, mobile phones etc. that were lost or stolen, confiscated, and so on. The officer checks at high speed whether the passport in question actually contains one of the material or personal findings listed here as hits. She now checks the passport: she goes through all the pages to see where and which stamps are in the document . . . Once this is done, the officer asks: 'Where do you come from?' 'Why do you come to Germany?' 'How long do you want to stay?' 'What is your job?' (border guard 2)

Although the key filtering interest in the field of airport security at large is to detect possible threats by detecting 'hidden criminal intentions during the build-up phase' (Koller, Wetter, and Hofer 2015, 683), for border guards this is combined with other detection aims, such as visa overstays, document fraud or open arrest warrants. With all travellers that go through the passport check, they must search for evidence of forged documents. As the field note shows, border guards enact their authority in a limited space with high technological density that manifests in information from the databases they must check, which asks for a lot of the officers' attention during the interaction with the passenger. The filtering here is reassessed by the police, also because the level of sensitivity of the computational filtering system is at times so roughly configured that there is a constant alert for most travellers (see also Bonelli and Ragazzi 2014, 480 for the consistency of low-tech anticipatory practices). They must check whether the computer's alerts are correct, which, as Leese and Pollozek (2023, 8) describe, contradicts the paradigm of efficient interventions through data at the airport. In order to clarify their initial observation from the alert, they combine the information with statements from the traveller in a check on 'plausibility'.[16]

Even in the face of information that fits the criteria of 'low risk' (see Molotch 2014, 103), when they have doubts, the border guards will ask for further proof. Here we witness a change from databank-driven profiling to a form of argument that addresses the truthfulness of the role of the harmless passenger. They attempt to uncover narrative inconsistencies or incongruities in the passenger's narrative behaviour. The *fact*-like information is then contextualised by a verbal statement in an often-similar communicative process structure: starting with the question of the origin of a flight, something which is known information to the officers, from which they move on to

[16] Equally plausibility is a cue within laboratory research on intent detection, see Vrij et al. 2011.

increasingly unknown terrain, like 'What is the reason for your stay?' (several border guards). Similar to what Jörg R. Bergmann (1993, 305–6) reveals in his analysis of the communication structure of fire department emergency calls, follow-up-questions from the border guards mainly serve to verify the truth, even in the mode of small talk, in which phatic elements of communication come to the fore. And here, surrounding these two filtering aspects, a third one emerges: the sense of the police officer that there is an implausibility, which first and foremost unfolds as discrepancies between the person's appearance and the information she/he provides. Contrary to how Harvey Molotch (2014, 115) describes it, in this security regime a whole range of information that comes from routine interactions such as small talk and jokes, which we often observed, is not eliminated into 'irrelevant topics'. It rather generates the base for their sensing (im-)plausibilities for which gaze avoidance, or speaking too late or slowly when asked something, stand as examples (several border guards).

This kind of observation of travellers' behaviour relies on their experience and professional training. It guides their actions, which in light and in view of the high cognitive and time demands that the computer processing of passengers entails, cannot be characterised as an 'atrophy of vigilance' (ibid., 106). So here, besides the explicable indicators, resides an un-explicated context of knowledge that is based on their expertise. This is when what is seen as implausible cannot be explicated. Sometimes the missing plausibility comes from a contradiction of the expected norm. In this regard, all persons in the field of border control emphasised the rationale of situational baselining to be of key relevance to their work. Even though the security actors dealt with each person individually, the baselining in this field could only be one that was oriented on collective behaviour. This meant that the usual behaviour, attendance, staffage etc., at a specific time and place of the airport is taken as a norm for this field. Here the necessity of clarification is also referred to as 'something doesn't feel right' (several border guards) or 'something doesn't make sense' (border guard 5), meaning that plausibility is attributable to 'common sense' or familiarity with the environment (several border guards). As Collins (2007, 261) notes, this kind of knowledge is 'knowledge belonging to communities' and therefore it 'is beyond the control of the individuals within the communities'. The information is assessed by the 'human cognitive system operating as the filter' (Razghandi and Yaghmaei 2020) and this kind of 'gut feeling' (several border guards) refers to multisensory sources of immediate knowledge, entangled with interactions and observations of passengers. Observations play a crucial role in their anticipation of indicators for harmful intent, but it is situated: observation always takes place during the interaction, but sometimes it is also more future-related, as for example when they peek through the glass pane gaining an impression of the passengers waiting in line and anticipating what to expect. The sorting process of letting some people pass while others need to be scrutinised further inherits rationales, and is partly data-driven – a knowledge base which can be made explicit, but must be assessed and overruled by a less-explicable form of filtering. The overruling that we observed confirms what Teresa Degenhardt and Mike Bourne emphasise in their account of the 'human ability to suspect', when the border guards in their study do not trust technology 'to identify crucial differences that can be 'sensed'' (2020, 216).

Airport Security Screeners: '*Something's Missing*'

The workplace of airport security screeners forms a specifically shaped architectural microcosm that guides their search for clues to suspicion. As with the border control, it is a technologically dense environment (see also Bassetti 2017), but the diverse mini-checkpoints, where passengers and hand luggage are searched, are spread over a larger area. These stations include the hand baggage drop-off at the entry of the passenger screening; the body scanner and the manual search for dangerous objects on the passengers' bodies; the baggage screening using X-rays and the assessment of the resulting 2- or 3D images by the airport screeners, and the manual baggage check, which are supplemented by random wipe tests for explosive materials. In this kind of pre-scripted setup, the technical devices, passengers and their carried objects are transformed into epistemic objects (Linhardt 2000, 85). The multitude of instruments provides for a 'close sensing' in which machine vision is supplemented with the human touch (Parks 2007, 190)

Often the technical output provides orientation for further action. For example, if a test for explosives is positive, a specific sequence of separate control measures is carried out: the passenger's body is manually examined again, the federal police are informed, databases are queried, boarding passes are inspected and cameras are activated. This seemingly objective action orientation of the test for explosives is contested, because it results from the fact that certain beverage containers cannot be examined by the devices used for explosive trace detection and certain liquids cannot even be recognized. Thus, the decision if further action is recommended is subject to negotiation. This process, although intended to objectify suspicion (Linhardt 2000, 103), can also create surplus meaning. In this context, it becomes apparent that also the X-ray images of the passengers' baggage can open up disruptive possibilities:

> After returning [from the baggage drop-off station], Dana now sits at the hand-baggage screen after standing for a long time. In an image she sees an object (small, square with several components) that she 'doesn't like at all'. Her colleague sees it the same way. Dana calls the module manager and shows him the item. He asks if she has already spoken to the passenger. She denies this. He says that's what he would do first to clear it up. Dana points to the image again and says that it has everything it needs for a red button [highest level of alarm] and that she is inclined to press red. 'Nothing is missing', she says. . . . The module manager, on the other hand, says that he is missing something. He can't describe it, but he is missing something. He then goes to the passenger, who is American, and lets her tell him what it is that they are seeing. The passenger replies: An E-cigarette, which immediately seems plausible to him. He says to Dana how good it is if you can clarify this directly with the passenger. (security screener 77)

This sequence contains two aspects that guide the practice of airport screeners: firstly, the plausibility check with which the ambiguity of the threat indicator is decomposed as harmless in a friendly conversation, instead of initiating the highest alarm, which would initiate a number of security measures, including the closure of the area. The frequently observed plausibility checks are characterised by 'calming', as emphasised by Molotch (2014, 122). Herein the security screeners handle their 'mission ambivalence' (Bassetti 2017, 2) between being alarmed and their role as service personnel, who ensure a good experience for passengers, in favour of the latter.

Interactions as such become necessary, secondly, only because of the inexplicability, which functions as both an indication of a threat and of its harmlessness – refuting the thesis of the democratic nature of control through technology (as in Linhardt 2000). This refers to an idea of normality that cannot be made explicit. When they are at the hand baggage screen to evaluate the images, baselining relates to what is identified as common, normal, and to what fits together. But in this case knowledge refers less to explicable reasons than to a feeling that finds its reference in vast recollection of previous experience. The sense 'of not liking this at all' or 'feeling in the stomach' (several security screeners) serves as a guide throughout the situations, or irritations of some kind, in which their sensual impression was trusted as a worthwhile signal for an indicator. It stems from attention to verbal, tactile and visual details[17] – including facial expressions, movements and side conversations, which form the reference for what can be described as a sense of normality and proves to be a collective situational baseline for suspicious behaviour in this context. Most of the screeners have their own theory about the passenger, which finds their core in behaviour patterns that sometimes deviate from the baseline, such as strong agitation, too obvious calmness or inappropriately loud behaviour. But often these explicit cues are also questioned, not only because of their indexicality, but also what has been learned via security handouts[18] often contradicts their experience, as one screener told us several times: 'You have to discard how you were drilled' (security screener 77).

When Collins (2007, 258–59; 2010, 99–117) explains his concept of somatic tacit knowledge, he argues that there are guided rules that could be made explicable but that in the moment of action are troublesome to use or have present. Working in the airport security (and border control) context requires a constant observation and assessment of people, objects, and situations in light of what a security actor perceives to be the normative expectation for the specific time and place. Therefore, the security personnel have to stay immersed in society, and gain knowledge of what is seen as a commonality in daily utensils (like what an up-to-date hair dryer looks like) in order to interpret the changing images, they see.

Automation Research and Development: '*The Data is There*'

While there has been some on-site testing of intent detection systems, as in the aforementioned projects, the dominant search for automated solutions still takes place in the laboratory. Scientists from various fields (e.g. applied psychology, computational science) engage in research on the

[17] See Parks study on airport screeners with an emphasis on the visual aspects in the 'labour of searching for something' (2007, 187).

[18] For security reasons we had no access to the service agreement for the airport screeners, in which rules for the practice are formulated. As we know from our ethnographic conversations, at least in the past, the service agreement also included information about which behaviour-based characteristics the screeners should pay attention to.

automation of intent detection relying on the measurement of physiological characteristics. The narrative of one researcher who developed a system based on facial cues (having a background in mathematics) represents many of the aspects that can be considered a common core in this field:

> So what machine learning does is that you can extract certain features as we call them. So, for example, let's just say: you['ve] got 2,000 people who lied okay. And you've got their facial expressions, their emotions, their blood flow pattern, their thermal everything. That data is there. And there must be some features. . . . the timing of the answer or some facial expression, the blink rate. That kind of thing. . . . You collect a bunch of data. You assume there is some sort of separation between these data sets and then you train whatever sort of algorithm. . . . And then we essentially just throw those features into our algorithm. And the algorithm will say, 'actually these features belong in that class'. Lie class. (researcher 6)

This excerpt does not just outline the basic idea that deception, framed as deviation from normal behaviour, can be determined by means of machine learning techniques (see e.g. Khan et al. 2021; O'Shea et al. 2018; Elkins et al. 2018) via classifications, but it also illustrates how *intent* is conceptualised for automated detection, starting with machine learning. The central rationale of this filtering process is that of *ground truthing*. In the context of automation, it is based on the idea of a quasi-natural truth that is to be found in the data, 'that belong in that class'. Ground truth emerges from content, for example images seeped in the system, which is to learn to recognize them, transforming 'content into data that computers can process' (Aradau and Blanke 2015, 3). The system is supposed to recognise differences within new content to enable it to automatically define normalcy from the intent to deceive, or in the words of researcher 6 it is expected to figure out 'the changes that happen on the facial [expressions]'. Here, the decisive criteria of assessing the veracity of a person are located in physical, bodily manifestations: like 'facial expressions, their emotions, their blood flow pattern' (researcher 6). These cues are not only representing, but predetermining for example, what a face looks like when one is speaking or hiding the truth, what emotions are felt, or which bodily behaviour is indicating deceit. Here explicit knowledge emerges[19] – especially regarding the cues on which the identification is based. The overall result is the creation of facticity. The underlying *ground truthing* process can be described as creating invariable ground 'truth excerpts' (researcher 13). This phrasing of the field sheds light on how the intention to deceive emerges through generalised deviations from normalcy and – in sharp contrast to baselining – through abstraction from the situation. In computational research, the reasoning is called the *ground of truth* on which certainty is based that a specific person's reaction can be clearly explained only in terms of the stimulus in question respectively by defined specific proxy features indicating the intent to deceive. This

[19] As implicit knowledge that cannot be algorithmically defined (such as social norms or collective practices), information must always be converted into an explicit form.

capability of the system is seen in the sheer amount of data to which algorithms can be applied, or as researcher 6 termed it above, 'that data is there'.

But machine learning does not create suspect categories. Instead, it works on the binarization of data that is used to train models. Therefore, changing our perspective now to the implicit dimensions of ground truthing in automated deception already on a semantic level, the interviewees' continuation of this process – assuming that "there is some sort of separation between these data" (Jaton 2021, 272), points to the decision-making processes in this approach to make this data actionable, which is 'time consuming human work'. Especially within the practice of annotating or labelling data, which later serves as training data, we can observe how humans and machines are brought together in the same infrastructures to process the data. Stemming from a research field in which we were shown and explained how annotations of body postures were done – both manually and via algorithm, the following description of one researcher sheds light on how difference-distinctions are construed that can lead to a classification system of *harmful intent*:

> So it's really this question of how much time do I give myself and how many resources. If I have an unlimited budget and manpower, I can't really say whether everything is impossible. However, it is often always a compromise at this point and in theory it is assumed that an ensemble of people should be able to reach an objective truth. Of course, there are problems where humans are not that well suited, with machines, temperatures, etc., where we have better sensors than humans. With exactly this task that concerns me, which involves detecting people, estimating poses and recognizing activity. Purely theoretically, you can find a point where you are objectively understood, that is, that you have caught the truth or have reached a tolerance range, that is the truth. (researcher 13)

As we can see, annotating or labelling data varies with interpersonal situations, interactional norms, and local agreements (and as Degenhardt and Bourne point out, scientists also integrate their 'gut feeling' in the work, 2020, 218). It is based on problem knowledge, which can be characterised as implicit and ambiguous or in Collins's words socially 'embedded' (2010, 11). As its situational rules are open to negotiation, the achievement of objectivity is redefined into a mere theoretical aim. Here we see, just like Linhardt (2000, 95) emphasised, that a normalcy is materialised. The question of what counts as an indicator of harmful intent directly points to what Collins (2010, 91) calls the 'contingency' problem, of why this knowledge is not explicated: a specific professional experience as well as power relations that obfuscate the practice and choices made that add to the potentially harmful consequences of problem definition and training data (see Barocas and Selbst 2016).

The contingency-problem can also be attributed to the constant accumulation of data, as a final aspect of the implicit knowledge dimension of the filtering. As enormous databases that everybody can use is the ultimate dream of researchers in this field, existing databases are an additional source for the identification of cues. Stemming from heterogenous research, for example on EEG-data or remote photoplethysmography (see Speth et al. 2021), and various epistemological backgrounds, matching those databases, if publicly available, results in a conglomeration of data that do not have much in common, due to the various cues that are placed as indicative of deception.

Configuring Towards a Hermeneutics of Suspicion

Filtering is a fundamental technique by which both human and non-human actors shape their environment through differentiation. As such, the article engages with an exemplary case of the anticipated transformative potential of automation (as highlighted by Potthast, Jobard and Linhardt) that not only justifies its integration into security technologies, but, as O'Grady (2021) emphasises, allows us to take a closer look at the epistemological reasons for automation, which has an increasingly significant influence on filter decisions made in an progressively more data-driven society. In outlining the epistemological differences of *baselining* and *ground truthing*, we see that both rationales involve tacit as well as explicit knowledge, but the way norms and deviation are captured contrasts sharply.

What became evident in our research is the relevance of situated knowledge, of which the tacit is an essential element. As Molotch (2014, 88) reminds us, the entire 'human variation in physical form as well as in biographical contingencies' appears at the checks to be scrutinised for actionability. While it is the border guards and screeners task to respond to travellers (service imperative) and at the same time anticipating threats (security imperative), they have to acknowledge the idiosyncrasies within the broad range of humanity. Security actors therefore use multiple layers when investigating the situation, trying to achieve plausibility. This is unlike machine-centred procedures that lack situative flexibility.

Therefore, the rationales of situational *baselining* can be characterised, as by Collins, as improvisation, whereby *ground truthing* follows a logic of composition. Although automated detection systems are key to the anticipatory logic to overcome the limits of knowledge by anticipating possible futures (see Amoore 2013) in their reference and fixation on data from the past, they lack the ability to adapt themselves to different environments or situations, respectively elements that are created in situ. In comparison, improvisation is a reaction in the present to the unpredictable, and occurs in the situation itself.

Although human rationales are reflexive, performative and context-dependent, they co-produce a referential context centred on the idea that one accessible truth, in this case the deviation of the situational base at the airport, is for a large part based on non-verbal behaviour. This is a commonality in the otherwise heterogeneous fields that pursue contrasting approaches to *truth accountability*. But this is even more the case within the envisioned automated intent detection, where these foci form the implicit base but are encapsulated within the situated classification. Even though our study captured different rationales between human- and machine-centred filtering procedures, they all inherit shared moments and visions which Bigo and Tsoukala (2008, 23) refers to as a 'de-differentiation' in this sphere: they produce knowledge about an environment that they are simultaneously bringing into life and foster a belief that there is a way to detect the truth about one's intentions.

To summarise, while human filtering through baselining is accused of being biased, the informational, machine-centred systems are hoped to be based on more neutral grounds (as in Jobard

and Linhardt 2008; Potthast 2011). But automated filters are prone to their own way of producing discriminatory referencing systems through reproduction. While there is an ascertained inscription of normality in the sociomaterial assemblages, we concede that the more human-centred actions within security work are replaced by automated systems, the more physiological cues will dominate the hermeneutics of suspicion at work. Tinkering with these systems through drafting machine-centred intent detection has a reality constituting effect that eliminates contextuality and the acknowledgement of human diversity. It is presented as a remedy, a promise of truth verifications to provide security which is more important than the reliability of the detection system, as Melissa Littlefield (2011, 10) showed in her work on lie detectors and their successors. The anticipated ontology of security, normality and deviance, and the perception of threats to which a device offers a solution, is mediated in the research process that our participants reflect upon. Therefore, our research can be understood as a contribution to the STS engagement with the bias of automated systems. Thus, we sensitise for the concomitant that harmful intent as a nonverbal physiological inscription manifests as an epistemological object, as well as a single truth in suspicion practices, since the contingencies that the fields showed were not putting the idea of intent detection into question. In our view, it would be worthwhile for STS research to engage not just more intensively with security technologies per se, but to relate the claim of objectivity, when it comes to machine-centred procedures, to the imagination of its object, in our case that of *intent*. In the end, we are confronted with the question of how these developments could reconfigure our society.

Acknowledgements

We are grateful to the editorial collective and the anonymous reviewers for their comments on previous versions of the paper, as well as to Larissa Fischer, Torsten Voigt, Ben Hiscox and Milena Rössner for their support. Our special thanks go to all those in the research field, the airport and aviation security who kindly agreed to talk to us and let us accompany them in their work even though we came amid the burdened Corona-time.

Author Biography

Bettina Paul teaches criminology at the University of Hamburg, Germany. Her research is inspired by the intersection of STS and anticipatory truth verification systems.

Sylvia Kühne is a sociologist and criminologist with a special research focus on the logic and consequences of emerging technologies.

References

Aas, Katja Franko, Helene Oppen Gundhus, and Heidi Mork Lomell, eds. 2009. *Technologies of InSecurity: The Surveillance of Everyday Life*. Abingdon: Routledge-Cavendish.

Adey, Peter. 2004. "Surveillance at the Airport: Surveilling Mobility/Mobilising Surveillance." *Environment and Planning A: Economy and Space* 36(8): 1365–80. https://doi.org/10.1068/a36159.

———. 2006. "If Mobility Is Everything Then It Is Nothing: Towards a Relational Politics of (Im)Mobilities." *Mobilities* 1(1): 75–94. https://doi.org/10.1080/17450100500489080.

———. 2009. "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body." *Environment and Planning D: Society and Space* 27(2): 274–95. https://doi.org/10.1068/d0208.

Amoore, Louise. 2009. "Lines of Sight: On the Visualization of Unknown Futures." *Citizenship Studies* 13(1): 17–30. https://doi.org/10.1080/13621020802586628.

———. 2013. *The Politics of Possibility: Risk and Security Beyond Probability*. Durham: Duke University Press.

———. 2019. "Doubt and the Algorithm: On the Partial Accounts of Machine Learning." *Theory, Culture & Society* 36(6): 147–69. https://doi.org/10.1177/0263276419851846.

Aradau, Claudia, and Tobias Blanke. 2015. "The (Big) Data-Security Assemblage: Knowledge and Critique." *Big Data & Society* 2(2): 1–12. https://doi.org/10.1177/2053951715609066.

Aradau, Claudia, and Rens Van Munster. 2007. "Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future." *European Journal of International Relations* 13(1): 89–115. https://doi.org/10.1177/1354066107074290.

Barocas, Solon, and Andrew D. Selbst. 2016. "Big Data's Disparat Impact." *California Law Review* 104(3): 671–732. https://doi.org/10.15779/Z38BG31.

Bassetti, Chiara. 2017. "Airport Security Contradictions: Interorganizational Entanglements and Changing Work Practices." *Ethnography* 19(3): 288–311. https://doi.org/10.1177/1466138117696513.

———. 2021. "The Tacit Dimension of Expertise: Professional Vision at Work in Airport Security." *Discourse Studies* 23(5): 597–615. https://doi.org/10.1177/14614456211020141.

Bechmann, Anja, and Geoffrey C. Bowker. 2019. "Unsupervised by Any Other Name: Hidden Layers of Knowledge Production in Artificial Intelligence on Social Media." *Big Data & Society* 6(1): 1–11. https://doi.org/10.1177/2053951718819569.

Bergmann, Jörg. 1993. "Alarmiertes Verstehen: Kommunikation in Feuerwehrnotrufen. [Alarmed Making Sense: Communication in Fire Department Emergency Calls]." In *'Wirklichkeit' im Deutungsprozeß. Verstehen und Methoden in den Kultur- und Sozialwissenschaften* [Reality in the process of interpretation. Sense Making and methods in the cultural and social sciences], edited by Thomas Jung and Stefan Müller-Doohm, 283–328. Frankfurt am Main: Suhrkamp.

Biermann, André, and Stefan Kaufmann. 2021. "Sicherheit als epistemische Praxis in der Luftsicherheitskontrolle" [Security as an Epistemic Practice in Aviation Security Control]. In *Vielfältige Sicherheiten: Gesellschaftliche Dimensionen der Sicherheitsforschung* [Multiple Securities: Social Dimensions of Security Research], edited by Nicholas Eschenbruch, Stefan Kaufmann, and Peter Zoche, 159–82. Münster: LIT-Verlag.

Bigo, Didier, and Anastassia Tsoukala, eds. 2008. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, 11–19. First Edition. London: Routledge.

Bonelli, Laurent, and Francesco Ragazzi. 2014. "Low-Tech Security: Files, Notes, and Memos as Technologies of Anticipation." *Security Dialogue* 45(5): 476–93. https://doi.org/10.1177/0967010614545200.

Bourne, Mike, Heather Johnson, and Debbie Lisle. 2015. "Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies." *Security Dialogue* 46(4): 307–25. https://doi.org/10.1177/0967010615578399.

Collins, Harry. 2007. "Bicycling on the Moon: Collective Tacit Knowledge and Somatic-Limit Tacit Knowledge." *Organization Studies* 28(2): 257–62. https://doi.org/10.1177/0170840606073759.

———. 2010. *Tacit and Explicit Knowledge*. Chicago: The University of Chicago Press. https://doi.org/10.7208/chicago/9780226113821.001.0001.

Cubasch, Alwin J., Vanessa Engelmann, and Christian Kassung. 2021. "Theorie des Filterns: Zur Programmatik eines Experimentalsystems" [Theory of Filtering: About the Programmatic of an Experimental System]. Preprint. Zenodo: OpenAIRE, April 30, 2021. https://doi.org/10.5281/zenodo.4731045.

Degenhardt, Teresa, and Mike Bourne. 2020. "When Risks Meet: The Dance of Experience, Professional Expertise and Science in Border Security Technology Development." *Criminology & Criminal Justice* 20(2): 207–25. https://doi.org/10.1177/1748895818811896.

Denault, Vincent, Pierrich Plusquellec, Louise M. Jupe, Michel St-Yves, et al. 2020. "The Analysis of Nonverbal Communication: The Dangers of Pseudoscience in Security and Justice Contexts." *Anuario de Psicología Jurídica* 30(1): 1–12. https://doi.org/10.5093/apj2019a9.

Discern Science. N.d. Website. Accessed February 14, 2024. https://discernscience.com/.

Egbert, Simon, and Bettina Paul. 2018. "Moderne Verfahren der Lügendetektion als sicherheitspolitische Innovationen: Technikgenese zwischen diskursiven Versprechungen

und materialen Rückwirkungen" [Modern Methods of Lie Detection as Security Policy Innovations: Technology Genesis between Discursive Promises and Material Repercussions]. In *Diskursive Konstruktion und schöpferische Zerstörung: Begegnungen von Innovationsforschung und Diskursanalyse* [Discursive Construction and Creative Destruction: Encounters between Innovation Research and Discourse Analysis], edited by Saša Bosančić, Stefan Böschen, and Cornelius Schubert. Supplement, *Journal for Discourse Studies* S2: 129–159.

———. 2019. "Preemptive 'Screening for Malintent': The Future Attribute Screening Technology (FAST) as a Double Future Device." In "Socio-Technical Futures and the Governance of Innovation Processes – Sociological Perspectives," edited by Knud Böhle and Kornelia Konrad, special issue, *Futures* 109: 108–116. https://doi.org/10.1016/j.futures.2018.04.003.

Elkins, Aaron C., Elyse Golob, Jay Nunamaker, Judee Burgoon, et al. 2014. "Appraising the AVATAR for Automated Border Control: Results of a European Union Field Test of the AVATAR System for Interviewing and Passport Control. Conducted at the Henri Coandă International Airport, Bucharest, Romania, December 2013." A Report to FRONTEX, prepared by the National Center for Border Security and Immigration, and University of Arizona. October 2014, Accessed July 11, 2023. https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/002653/P9_RE(2019)002653(ANN3)_XL.pdf.

Elkins, Aaron C., Jeffrey G. Proudfoot, Nathan Twyman, Judy K. Burgoon, et al. 2018. "Embodied Conversational Agent-Based Deception Detection: Concealed Information Test Using Automated Electrodermal, Vocal, and Oculmentric Measurements." In *Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016. Volume 2*, edited by Yaxin Bi, Supriya Kapoor, and Rahul Bhatia, 294–307. Cham: Springer. https://doi.org/10.1007/978-3-319-56991-8_22.

Feijoo-Fernández, María Carmen, and Lucía Halty. 2018. "La intención es lo que cuenta: Una revisión sobre la detección del engaño en intenciones" [It's the Intention that Counts: A Review on Deception Detection Focused on Intentions]. *Papeles del Psicólogo/Psychologist Papers* 39(1): 51–59. https://doi.org/10.23923/pap.psicol2018.2849.

Feijoo-Fernández, María Carmen, Lucía Halty, and Andrés Sotoca-Plaza. 2023. "Like a Cat on Hot Bricks: The Detection of Anomalous Behavior in Airports." *Journal of Police and Criminal Psychology* 38: 72–82. https://doi.org/10.1007/s11896-020-09371-5.

Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement.* New York: New York University Press. https://doi.org/10.18574/nyu/9781479854608.001.0001.

Gillespie, Tarleton. 2014. "The Relevance of Algorithms." In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski,

and Kirsten A. Foot, 167–194. Cambridge, MA: MIT. https://doi.org/10.7551/mitpress/9780262525374.003.0009.

Gil-Fournier, Abelardo, and Jussi Parikka. 2021. "Ground Truth to Fake Geographies: Machine Vision and Learning in Visual Practices." *AI & Society* 36(4): 1253–1262. https://doi.org/10.1007/s00146-020-01062-3.

Glouftsios, Georgios, and Matthias Leese. 2023. "Epistemic Fusion: Passenger Information Units and the Making of International Security." *Review of International Studies* 49(1): 125–142. https://doi.org/10.1017/S0260210522000365.

Granhag, Pär Anders, and Erik Mac Giolla. 2014. "Preventing Future Crimes: Identifying Markers of True and False Intent." *European Psychologist* 19(3): 195–206. https://doi.org/10.1027/1016-9040/a000202.

Gulick, Walter B. 2023. "Machine and Person: Reconstructing Harry Collins's Categories." *AI & Society* 38: 1847–1858. https://doi.org/10.1007/s00146-020-01046-3.

Heinemann, Torsten, and Martin G. Weiß. 2016. "Biotechnologische Grenzregime" [Biotechnological Border Regimes]. In *An der Grenze: Die biotechnologische Überwachung von Migration* [At the Border: The Biotechnological Surveillance of Migration], edited by Torsten Heinemann and Martin G. Weiß, 7–21. Frankfurt: Campus.

Honts, Charles R., and Maria Hartwig. 2014. "Credibility Assessment at Portals." In *Credibility Assessment: Scientific Research and Applications*, edited by David C. Raskin, Charles R. Honts, and John C. Kircher, 37–61. San Diego: Academic Press. https://doi.org/10.1016/B978-0-12-394433-7.00002-6.

Jasanoff, Sheila. 2015. "Future Imperfect: Science, Technology, and the Imaginations of Modernity." In *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, edited by Sheila Jasanoff and Kim Sang-Hyun, 1–33. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226276663.003.0001.

Jaton, Florian. 2017. "We Get the Algorithms of Our Ground Truths: Designing Referential Databases in Digital Image Processing." *Social Studies of Science* 47(6): 811–40. https://doi.org/10.1177/0306312717730428.

———. 2021. *The Constitution of Algorithms: Ground-Truthing, Programming, Formulating*. Cambridge, London: MIT Press. https://doi.org/10.7551/mitpress/12517.003.0021.

Jobard, Fabien, and Dominique Linhardt. 2008. "The Check and the Guardianship: A Comparison of Surveillance at an Airport and a Housing-Estate Area in the Paris Outskirts." In *Surveillance and Governance: Crime Control and Beyond*, edited by Mathieu Deflem, and Jeffrey T. Ulmer, 75-100. Leeds, UK: Emerald. https://doi.org/10.1016/S1521-6136(07)00204-7.

Jupe, Louise M., Sharon Leal, Aldert Vrij, and Galit Nahari. 2017. "Applying the Verifiability Approach in an International Airport Setting." *Psychology, Crime & Law* 23(8): 812–25. https://doi.org/10.1080/1068316x.2017.1327584.

Jupe, Louise M., and David A. Keatly. 2020. "Airport Artificial Intelligence Can Detect Deception: Or Am I Lying?" *Security Journal* 33: 622–635. https://doi.org/10.1057/s41284-019-00204-7.

Khan, Wasiq, Keeley Crockett, James O'Shea, Abir Hussain, et al. 2021. "Deception in the Eyes of Deceiver: A Computer Vision and Machine Learning Based Automated Deception Detection." *Expert Systems with Applications* 169: 1–15. https://doi.org/10.1016/j.eswa.2020.114341.

Kleinberg, Bennett, Arnoud Arntz, and Bruno Verschuere. 2019. "Detecting Deceptive Intentions: Possibilities for Large-Scale Applications." In *The Palgrave Handbook of Deceptive Communication*, edited by Tony Docan-Morgan, 403–27. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-96334-1_21.

Knoblauch, Hubert. 2001. "Fokussierte Ethnographie" [Focused Ethnography]. *Sozialer Sinn* 2(1): 123–42. https://doi.org/10.1515/sosi-2001-0105.

Knorr, Karin D. 1979. "Tinkering Toward Success: Prelude to a Theory of Scientific Practice." *Theory and Society* 8: 347–76. https://doi.org/10.1007/BF00167894.

Koller, Corinne I., Olive E. Wetter, and Franziska Hofer. 2015. "What Is Suspicious When Trying to Be Inconspicuous? Criminal Intentions Inferred from Nonverbal Behavioral Cues." *Perception* 44(6): 679–708. https://doi.org/10.1177/0301006615594271.

Krasmann, Susanne. 2003. *Die Kriminalität der Gesellschaft: Zur Gouvernementalität der Gegenwart* [The Criminality of Dociety: On the Governmentality of the Present]. Konstanz: UVK.

Krüger, Jenny K. 2019. "Polizeiliche Verhaltenserkennung: Die Grundlagen" [Police Behavioural Detection: The Basics]. In *Zukunft der Polizei: Trends und Strategien* [Future of the Police: Trends and Strategies], edited by Hans-Jürgen Lange, Thomas Model, and Michaela Wendekamm, 189–208. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-22591-9_13.

Kurt, Ronald. 2008. "Komposition und Improvisation als Grundbegriffe einer allgemeinen Handlungstheorie" [Composition and Improvisation as Basic Ideas of a General Action Theory]. In *Menschliches Handeln als Improvisation: Sozial- und musikwissenschaftliche Perspektiven* [Human Action as Improvisation: Social and Musicological Perspectives], edited by Ronald Kurt and Klaus Näumann, 17–46. Bielefeld: Transcript Verlag. https://doi.org/10.1515/9783839407547-001.

Leese, Matthias, and Silvan Pollozek. 2023. "Not So Fast! Data Temporalities in Law Enforcement and Border Control." *Big Data & Society* 10(1): 1–13. http://doi.org/10.1177/20539517231164120.

Lehr, David, and Paul Ohm. 2017. "Playing with the Data: What Legal Scholars Should Learn about Machine Learning." *UC Davis Law Review* 51(2): 653–717. Accessed July 4, 2023. https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Lehr_Ohm.pdf.

Linhardt, Dominique. 2000. "Demokratische Maschinen? Die Vorrichtung zur Terrorismusbekämpfung in einem französischen Großflughafen (Paris-Orly)" [Democratic Machines? The Counter-Terrorism Device at a Major French Airport (Paris-Orly)]. *Kriminologisches Journal* 32(2): 3–4. 82–107.

Littlefield, Melissa M. 2011. *The Lying Brain: Lie Detection in Science and Science Fiction*. Ann Arbor, MI: University of Michigan Press. https://doi.org/10.3998/mpub.3091709.

Lyon, David. 2008. "Filtering Flows, Friends and Foes: Global Surveillance." In *Politics at the Airport*, edited by Mark B. Salter, 29–50. Minneapolis, MN: University of Minnesota Press. https://www.jstor.org/stable/10.5749/j.ctttsqsx.6.

Magnuson, Stew. 2008. "Transportation Lab Seeks Radical Change at Airport Checkpoints." *National Defense Magazine*, March 1, 2008. Accessed February 26, 2024. https://www.nationaldefensemagazine.org/articles/2008/2/29/2008march-transportation-lab-seeks-radical-change-at-airport-checkpoints.

Molotch, Harvey. 2014. *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*. New Jersey: Princeton University Press. https://doi.org/10.1515/9781400852338.

Musik, Christoph. 2016. "Ground Truth Studies: A Socio-Technical Framework." *Recent Advances in Multimedia Processing, Organization and Visualization beyond Domains and Disciplines*, 10. Forschungsforum der österreichischen Fachhochschulen [Tenth Research Forum of the Austrian Universities of Applied Sciences]. https://doi.org/10.13140/RG.2.1.3577.1284.

Musik, Christoph, and Matthias Zeppelzauer. 2018. "Computer Vision and the Digital Humanities: Adapting Image Processing Algorithms and Ground Truth through Active Learning." *VIEW Journal of European Television History and Culture* 7(14): 59–72. https://doi.org/10.25969/mediarep/14754.

Nunamaker Jr., Jay F., Judee K. Burgoon, and Justin Scott Giboney, eds. 2016. "Special Issue: Information Systems for Deception Detection." *Journal of Management Information System* 33(2): 327–331. https://doi.org/10.1080/07421222.2016.1205928.

O'Grady, Nathaniel. 2021. "Automating Security Infrastructures: Practices, Imaginaries, Politics." *Security Dialogue* 52(3): 231–48. https://doi.org/10.1177/0967010620933513.

O'Shea, James, Keeley Crockett, Wasiq Khan, Philippos Kindynis, et al. 2018. "Intelligent Deception Detection through Machine Based Interviewing." *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://doi.org/10.1109/IJCNN.2018.8489392.

Parks, Lisa. 2007. "Points of Departure: The Culture of US Airport Screening." *Journal of Visual Culture* 6(2): 183–200. https://doi.org/10.1177/1470412907078559.

Pollozek, Silvan, and Jan-Hendrik Passoth. 2024. "Devices of Suspicion: An Analysis of Frontex Screening Materials at the Registration and Identification Center in Moria." *Journal of Ethnic and Migration Studies* 50(9): 2327–2345. https://doi.org/10.1080/1369183X.2024.2307786.

Potthast, Jörg. 2011. "Sense and Security: A Comparative View on Access Control at Airports." *Science, Technology & Innovation Studies* 7(1): 87–106. Accessed December 19, 2024. https://sti-studies.com/wp-content/uploads/2019/11/7.1-sense.pdf.

———. 2016. "Luftraumsoziologie: Flughäfen als Herausforderung für eine Theorie sozialer Praktiken" [Airspace Sociology: Airports as a Challenge for a Theory of Social Practices]. *Soziologie* 45(2): 127–47. Accessed December 19, 2024. https://publikationen.soziologie.de/index.php/soziologie/article/view/858/1113.

Razghandi, Khashayar, and Emad Yaghmaei. 2020. "Rethinking Filter: An Interdisciplinary Inquiry into Typology and Concept of Filter, Towards an Active Filter Model." *Sustainability* 12(18): 7284. https://doi.org/10.3390/su12187284.

Salter, Mark B., ed. 2008. *Politics at the Airport*. Minneapolis, MN: University of Minnesota Press. https://www.jstor.org/stable/10.5749/j.ctttsqsx.5.

Sánchez-Monedero, Javier, and Lina Dencik. 2020. "The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl." *Information, Communication & Society* 25(3): 413–430. https://doi.org/10.1080/1369118X.2020.1792530.

Schäufele, Fabia. 2017. *Profiling zwischen sozialer Praxis und technischer Prägung: Ein Vergleich von Flughafensicherheit und Credit-Scoring* [Profiling between Social Practice and Technical Characterisation: A Comparison of Airport Security and Credit Scoring]. Wiesbaden: Springer. https://doi.org/10.1007/978-3-658-16969-5.

Schouten, Peer. 2014. "Security as Controversy: Reassembling Security at Amsterdam Airport." *Security Dialogue* 45(1): 23–42. http://www.jstor.org/stable/26292273.

Speth, Jeremy, Nathan Vance, Adam Czajka, Kevin W. Bowyer, et al. 2021. "Deception Detection and Remote Physiological Monitoring: A Dataset and Baseline Experimental Results." 2021 IEEE International Joint Conference on Biometrics (IJCB), Shenzhen, China, 1–8. https://doi.org/10.1109/IJCB52358.2021.9484409.

Suchman, Lucy. 2007. Human-Machine Reconfigurations: Plans and situated actions (2nd edition). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511808418.

———. 2023. "Imaginaries of Omniscience: Automating Intelligence in the US Department of Defense." *Social Studies of Science* 53(5): 761–86. https://doi.org/10.1177/03063127221104938.

Sutrop, Margit, and Katrin Laas-Mikko. 2012. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics." *Review of Policy Research* 29(1): 21–36. https://doi.org/10.1111/j.1541-1338.2011.00536.x.

Tavory, Iddo, and Stefan Timmermans. 2014. *Abductive Analysis: Theorizing Qualitative Research*. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226180458.001.0001.

Trauttmansdorff, Paul. 2022. "Borders, Migration, and Technology in the Age of Security: Intervening with STS." *Tecnoscienza: Italian Journal of Science & Technology Studies* 13(2): 133–54. https://doi.org/10.6092/issn.2038-3460/17584.

Verschuere, Bruno, Chu-Chien Lin, Sara Huismann, Bennett Kleinberg, et al. 2023. "The Use-the-Best Heuristic Facilitates Deception Detection." *Nature Human Behaviour* 7: 718–728. https://doi.org/10.1038/s41562-023-01556-2.

Vrij, Aldert. 2008. *Detecting Lies and Deceit: Pitfalls and Opportunities*. Second Edition. West Sussex: John Wiley & Sons Ltd.

Vrij, Aldert, Maria Hartwig, and Pär Anders Granhag. 2019. "Reading Lies: Nonverbal Communication and Deception." *Annual Review of Psychology* 70: 295–317. https://doi.org/10.1146/annurev-psych-010418-103135.

Vrij, Aldert, Sharon Leal, Samantha Ann Mann, and Pär Anders Granhag. 2011. "A Comparison between Lying about Intentions and Past Activities: Verbal Cues and Detection Accuracy." *Applied Cognitive Psychology* 25(2): 212–18. https://doi.org/10.1002/acp.1665.

Weydner-Volkmann, Sebastian. 2017. "Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm." In *Rethinking Surveillance and Control: Beyond the "Security versus Privacy" Debate*, edited by Elisa Orrù, Maria Grazia Porcedda, and Sebastian Weydner-Volkmann, 49–83. Baden-Baden: Nomos.