On security, once more.

Assorted inquiries in aviation.

Dissertation
zur Erlangung des Doktorgrades
der Wirtschafts- und Sozialwissenschaftlichen Fakultät
der Eberhard Karls Universität Tübingen

vorgelegt von

Matthias Leese, M.A.

aus Lörrach

Tübingen

2014

Tag der mündlichen Prüfung:	10.02.2015
Dekan:	Prof. Dr. rer. soc. Josef Schmid
1. Gutachter:	Prof. Dr. Thomas Diez
2. Gutachter:	Prof. Didier Bigo

On security, once more.

Assorted inquiries in aviation.

Matthias Leese

Table of Contents

Prelude: trajectory of a PhD project 4
I. Security 8
Foundations 10
Initial narrative: security as value 11
First narrative: security as transformation 13
Second narrative: security as securitization 17
Third narrative: security as future 21
Fourth narrative: security as government 26
Fifth narrative: security as surveillance 31
Sixth narrative: security as technology 35
Seventh narrative: security as economy 39
Eighth narrative: security as assemblage 43
II. Interlude 48
Stories from the airport 50
III. Analytics 55
Empirics 57
[Inquiry 1] 60
Blurring the dimensions of privacy? Law enforcement and trusted traveler programs 60
Security, risk, and privacy 62
From security governance to risk governance? 64
Context: disciplinary spaces 67
Conclusions: blurring the state and the market! 71
[Inquiry 2] 74
Humor at the Airport? Visualization, Exposure, and Laughter in the "War on Terror" 74
Laughter in the forbidden zone: empirical encounters 75
What we laugh at: different forms of humor 77
Mitigating conflict? 81
Zooming in closer on the body 83
Conclusions – exposure, shame, and the failure of affective engineering 85
[Inquiry 3] 88
Privacy and security – on the evolution of a European conflict 88
EU security research – on the emergence of a field and a conflict 88
Economics and technologies 90
A normative turn? 93
Privacy by design: a technological fix for a technological fix? 95

Conclusions ... 97
[Inquiry 4] ... 98
Body scanners in Germany: a case of failed securitization ... 98
Body scanners as securitization ... 98
The fragmented field of aviation ... 101
Studying technology ... 104
Conclusions ... 107
[Inquiry 5] ... 110
Governing airport security: an empirical account between economic rationality and the public good ... 110
Between necessary virtues and neutral nodes: security governance ... 111
High-risk, low-cost hybrids ... 112
Out-contracting along economic and political contexts: an empirical account ... 115
Economic trigger, causal chain ... 116
The political context and the public good ... 119
Conclusions: “more state, please”? ... 122
[Inquiry 6] ... 124
The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the EU ... 124
Aviation, risk, and PNR data ... 125
Theorizing profiling ... 127
Profiling and non-discrimination ... 129
The ‘new profiling’ as data-driven governance ... 130
Out of sight, out of mind? ... 134
Data-driven governance and non-discrimination ... 135
Conclusions ... 136
IV. Conclusions ... 139
The ‘so what?’ question ... 141
Last narrative: security as normativity ... 141
References ... 148

Prelude: trajectory of a PhD project

This could be a foreword. This could simply be a 'thank you' to all the people that have supported, inspired, rightfully criticized, or in some other way pushed forward my project of writing a thesis. Credit where credit is due, but this standard procedure has to wait until the end of this prelude, as it is supposed to be a little more than a simple foreword. First of all, it is supposed to clear the intellectual mess that has amounted in my head over the past three and a half years. Second, it is supposed to reflect the position of this thesis among the topology of academia. But mainly it is supposed be a brief genealogy – a look back at difficult, yet highly enjoyable times and a reflection about how, and through which particular processes and events, this thesis has evolved and at the same time changed its author – both in terms of disciplinary premises and a general stance towards academia itself. Hence, although by no means required in any university regulations, I seek here to retrace the *trajectory* of a PhD project.

The idea to reflect on that multi-year process that has led me up to this point has not entirely been my own, admittedly. *Flashback (1)*: February 2013, Stirling, Scotland: LiSS Doctoral School on Surveillance Studies. First day of class. William Webster discusses the actual process of planning and executing a PhD project and its embeddedness in a multitude of social (power) relations, institutional constraints and the increasing personal progress of getting a grip on both academic theory and the real world. During that session, William put forward one particular question that stuck in my head, and which is the main reason for writing this little reflection piece that is supposed to exceed the usual forewords that we find attached to the many theses published each year.

The question, paraphrased, was: "When eventually defending your thesis, and one of the committee members asks you whether you would have done anything differently in your work, what would be your answer?" Well, what if? The only right answer to such a question must obviously be: "Yes, of course – in hindsight I would have handled a lot of things differently. But only now do I know." Only in such fashion can you demonstrate that you are critical of your own work, that you are willing to admit mistakes and at the same time benefit from them, and that you are someone who cherishes the age-old method of learning through trial and error (which is a harsh, yet effective one, I guess). And however counter-factual that 'what if' question is, it is a great trigger to think about your choices, not only in ontological, epistemological, theoretical, methodological, and empirical terms – thus in the strict academic terms of your actual thesis – but also in terms of your individual and institutional choices, of your personal encounters and inspirations, of your enjoyable and frustrating times as a young scholar. In short: about your own path of flight as part of academia.

One might be inclined to say that such a reflection necessarily includes a commitment to radical openness. As Brian Massumi (2002: 18) puts it: "If you know where you will end up when you begin, nothing has happened in the meantime. You have to be willing to surprise yourself writing things you didn't think you thought. […] This means you have to prepared for failure." Failure, that giant specter that haunts all of us young scholars – it certainly haunted me more than once. When Germany was struck by the discovery of academic fraud (primarily in terms of plagiarism) that reached (and still reaches) into the upper echelon of national and supranational politics – there was the specter of failure that made you question every single citation you ever inserted into one of your manuscripts. Every time I presented a piece of my work in front of a large audience (be it academics or practitioners) and it drew critical comments – there was the specter of failure that makes you question your smarts. Every time

I received crushing (and sometimes overtly hostile) reviews for a paper that I had submitted to a journal – there was the specter that insisted your writing was not good enough to ever perform at that level that was required in the competitive environment that is academia. Those specters and many more, they were ever looming on the horizon, just like the ominous 'event' that security politics strive to cancel out. An ironic parallel to the topic that I was concerned with in my work, admittedly. Yet all those specters, though numerous enough to fill a blockbuster horror-movie, served their purpose quite well. In the vein of both Massumi and the preemptive security politics of our times: they kept me *alert*.

Flashback (2): September 2013, Brussels, Belgium: EIRSS Summer School on borders, security, and mobility. Didier Bigo provides some feedback on a (in hindsight not so brilliant) piece that I had presented. The feedback, surprisingly, was quite benign, but one question did, once again, stick in my head. While I was arguing about rationalities and logics from a systems theoretic perspective, he asked whether I had adequately thought about the involved actor's trajectories. Well, in short: I had not – at least not adequately enough. Social trajectories, however, are just as important when it comes to academia as they are when it comes to empirical research. As Thomas Biersteker (2010: 602) puts it, particularly with regard to (critical) security studies, "we should ask questions about who funds our research, why that research is funded, for which audiences we are writing, and how our research either reinforces or challenges dominant scholarly research programs, doctrines, policy practices, and ideologies." Well, let's ask, then! Who did actually fund my research and what implications must be derived from such funding?

By the time I am writing this prelude, I have been involved in four different research projects – two of them funded within the security theme of the European FP7 framework, and two of them funded within the "high-tech strategy" of the German federal security research framework. This involvement has been both a blessing and a curse. Obviously, the grants paid my rent, which is not so bad for a start. Plus, they almost instantly got me in touch with the security research community – which is a strange breed of mostly engineers and a couple of social scientists and legal scholars uttering concerns about the new technologies to be developed (I am oversimplifying!) – that reflects the political program of security at the national and supra-national level. Moreover, the external funds freed me from any teaching obligations that eat up so much time of my fellow PhD candidates (in my third year, I opted to teach voluntarily nonetheless, but at this point I was already beginning to see the light at the end of tunnel). So much for the upside.

However, there is a downside. Put simply: you become part of the machine. The "security-industrial complex" machine, that is, in Ben Hayes' (2009) quite radical terms. The security research programs of both the FP7 framework and the German high-tech strategy feature a clear-cut economic agenda that has been shaped by the security industry in the first place. This is not a matter of moral corruption per se, but rather the acknowledgment of, most notably, the EU as a political union that has historically evolved through the desire to cooperate for the sake of creating wealth surplus. And nonetheless, the machine at times appears to be deeply stuck in a neo-liberal agenda that favors technological development regardless of social consequences. As David Harvey (2005: 68) puts it, "the neoliberal theory of technological change relies upon the coercive powers of competition to drive the search for new products, new production methods, and new organizational forms."

From the awareness of those mechanisms, I personally derived two consequences. First of all, I re-defined my own research agenda such that it now not only incorporates political and social

questions of 'security', but also political, social and economic questions of 'security research' – the latter often being the predecessor of the former. This is reflected by one of the analytical pieces of this PhD project ([Inquiry 3], the only one that is not directly concerned with aviation) that deals with the evolution of the presumed conflict between privacy and security. And second, I quickly learned to critically cherish the institutional frame that my own institution provides. The IZEW at the University of Tuebingen as a dedicated ethics institute occupies a rather awkward position within security research. On the one hand, ethical coverage within security research has been strengthened and is now mandatory under the European Horizon 2020 framework, but on the other hand, this turns you into the guy who could potentially red-flag the 'products' of research projects based on ethical concerns. And after all, the majority of your colleagues is likely to be composed of engineers, computer scientists, physicists and such who, according to my own experience, often see ethics more as a 'disturbance' than as a necessary virtue. As an institution, the IZEW has thus opted to enact an approach that our former colleague Michael Nagenborg (2009) has deemed "ethics as partner in technology development", seeking to implement social and ethical impact assessment early on and to establish an active dialogue with engineers and designers in order to avoid or at least mitigate detrimental social consequences of 'security'. In hindsight, this is something that for instance should have happened in the case of body scanner technology, as is pointed out in one of the analytical pieces of this thesis.

Being part of externally funded research projects, moreover – and this presumably was the most important impact for me personally – means that you get 'empirics-by-design'. Or rather: you can make use of synergy effects between empirical research that is conducted in the context of your everyday activities as part of a project team and your own analytical scope. And this is what I, of course, opted to do. Thus, the expert interviews and field observations that provided the empirical foundations for some of the analytical inquiries of this thesis were right in front of me, just waiting to be analyzed and connected to questions from the field of critical security studies.

Flashback (3): October 2013, San Diego, USA: 4S Annual Meeting. Small-talking to a colleague whom I had just met for the first time. Being asked what my PhD was about for arguably the hundredth time over the last couple years, I started my usual routine of explaining that my PhD project does not come in the classical shape of writing a book, but in a cumulative fashion that consists of a series of papers that are thematically connected, and that are either already published, accepted for publication, or even still under review at distinct journals. So far, so good. The response I got to that often-practiced explanation was not the usual one, however. She just nodded and said: "Oh, then you have like 10 supervisors, huh?" I had never really seen it this way, but there is certainly some truth in that statement. I definitely feel like I have largely benefited from being under review far more than I would have been during the process of writing a book.

Preparing a manuscript for submission to a journal, you are constantly forced to write at the highest level that is possible at the given moment – which in hindsight clearly pushed my limits. Also, you can manage to get a certain 'feel for the game' that is academia. There are wide debates about whether peer review would not empower (particularly senior and established) scholars to hide behind a protective veil of anonymity that allows them to defend their own research agendas while sabotaging others, but on the other hand, peer review is such an effective mechanism to receive feedback. As one colleague fittingly put it: "You can always use peer review processes and conferences as a test-bed, even if you feel that your

paper might still be flawed or is really not more than an initial idea." So I guess it's time to grind one's teeth and actually say thanks to all those people who have been going on my nerves with their nagging, their misunderstandings, their pointless proposals to "improve the quality of the manuscript" by turning it upside down and changing the core argument. After all, they *are* helping to improve the quality of the manuscript, because the force you to defend your arguments and thereby to sharpen them.

And since I have now incidentally started to say thanks, I shall continue to do so in a more proper fashion. I want to thank all of those who accompanied me through those last years – those who opted to engage with my ideas, those who went on to develop them with me, and most of all those who had the guts and the expertise to continually destroy, and then reconstruct them. In random order: Thank you Thomas for being the best supervisor imaginable. You have no idea how much of a role model you have been. Thank you Regina for always being supportive and for providing that necessary open space to pursue intellectual side strands apart from project work – and for finding money to keep me employed when two research grants were considerably delayed. Thank you Christian for making it clear early on that organization, efficiency, and output orientation are true academic game changers. More appreciation must go out to Michael and Tobias for numerous inspiring conversations. To Christina and Anja for being such great office mates and field research partners. To Birgit and Matthias for taking on the cold monster of bureaucracy. To Marijn and Nat for working stuff out together. To Marieke, Louise, and Didier for engaging with my work. And of course to everyone else whose names I have not mentioned here, however not forgotten, either.

And most of all thank you Elli – you know why.

I. Security

“My point is not that everything is bad, but that everything is dangerous, which is not exactly the same as bad. If everything is dangerous, then we always have something to do.”
(Foucault, 1984a: 343)

Foundations

There is no such thing as security. And yet security is a constituting part of our world. What at first glance appears as a glaring paradox, is in fact very much one of the central vanishing points of contemporary societies – both in political and social terms. As Anderson (2010b: 228) frames it, "security and securing are both dependent on nonexistent phenomena – threats and promises." And those threats and promises are where the political slips in, of course. In this introductory section to my PhD dissertation, I aim at unpacking the paradox of security and the way it plays out politically (and socially) through a variety of narratives. The narratives, yet capable of telling their respective distinct stories about security, must nonetheless be regarded as inextricably intertwined and overlapping. It could even be argued that they cumulatively build on each other in order to paint a more complete (and more problematic) picture of security. Once they will have been laid out and re-combined at the end of this section, the foundations for an understanding of security that thrives both on the impossibility of its very ontological existence and on its political transformations will become clear – or at least so I hope. The ensuing task will then be to use this framework to connect the analytical pieces that form the main section (III.) of this thesis. These 'assorted inquiries in aviation', which build the core of my project, are empirical takes on the politics and practices of security within a field that is often considered key for contemporary societies: aviation. As it embodies the time-space compression of globalization and the powerful desire for connectivity and mobility, aviation presents a prototypical field for the multiple narratives of security that will be told, and clearly points out their impact on the social – eventually leading to a necessary framing of the politicality of security as a normative question in section IV. With the eventual outlining of such a framework of normativity, I hope to put forward a modest contribution to the challenging of contemporary security politics and security practices, that at times stand in such a stark contrast to the fundamental values that the fluid concept of security originally was set to cherish and protect.

I aim not to solidify this fluidity. Security, almost by definition, perpetually escapes our attempts to grasp it and hold on to it. As such, security can be conceived of as an imaginary that can only exist *ex negativo* as opposed to something that threatens the fragile *status quo* in which we feel 'secure'. However, such threats are manifold, and in their social construction only limited by what indeed appears to be the limits of imagination – or what former US Secretary of Defense Donald Rumsfeld has infamously framed as "unknown unknowns." But only what is somehow known (or at least suspected) can be the target of precaution, prevention, and preemption – contemporary security politics have thus been dominated by the desire to identify threats, to calculate risks, and to harness and commodify the future in order to rid security of its persistently liquid character. Threatening events are simulated (Boyle and Haggerty, 2012), performed (Anderson and Adey, 2012), thought through (Anderson, 2010a; 2010b), driven by the media (Grusin, 2010; de Goede, 2008a), and, if need be, indeed just 'made up' (Salter, 2008b). Subsequently, the horizon of the manifold (in)securities we face today appears indeed a "politics of possibility" (Amoore, 2013), and as such is closely related to imagination.

Conceiving of security as a non-materiality then opens up a space to think about the multiple political transformations that security becomes subjected to. Or rather: how security is *imagined* throughout distinct theoretical and empirical registers. My aim here is not to add another layer to the multiple definitions of security, but to retrace and connect its potentialities that converge in my analyses in the broad field of aviation. There is a large and

ever-growing body of academic work that is continually concerned with those very questions, and countless spotlights have attempted to illuminate the shady nature of security. And yet, while particularly in critical security studies, once distinguished disciplinary discourses have started to merge, a considerable amount of (social scientific, broadly conceived) research on security still stands rather disconnected (Bigo, 2008a). In fact, "one finds people working on security and yet seemingly talking about very different things" (Neocleous, 2008: 6). I do in no way claim to build a definitive or even comprehensive link between these literatures here, but I feel that it is indeed helpful to consider the many ways that security has been researched as in order to add some brightness to the dispersed array of spotlights. Thus, I hope to both emphasize and connect the fragmented landscape of distinct perspectives in order to attempt to get a (temporary) grip on security. As Der Derian (1995: 28) frames the problematic, "the tension of definition is inherent in the elusiveness of the phenomenon it seeks to describe, as well as in the efforts of various users to fix and attach meanings for their own ends."

Subsequently, I have opted for a different way of approaching this shy phenomenon that is security. In order to theoretically underpin the empirical pieces of my thesis, this introductory section will tell a total of ten short narratives about security. The narratives feature distinct disciplinary roots, as well as a variety of ontological and epistemological assumptions that frame security according to a multiplicity of underlying rationalities, and, most of all, are connected to the perspectives that I have chosen to apply in my work. In no way does this selection of narratives claim to be complete or even indicate the possibility for completeness. Moreover, there is no specific linearity underpinning the narratives, although it could be argued that they 'complicate' matters throughout the process. However, they should rather be conceived of as a topological toolbox that increasingly fills as the theoretical foundations proceed. Thus, I seek to carve out major lines of inquiry for the manifold politicalities of security and to construct a solid basis for cross-references with my empirical pieces in order to engage "the ways in which security has been coined, shaped and deployed by political, commercial and intellectual forces" (Neocleous, 2008: 7). Put differently: I aim to tell a story of security through a variety of lenses, that, so much I hope at least, later on become reflected in the analytical part of this thesis.

Initial narrative: security as value

"A security threat is threatening precisely because it stems from what we value and what we fear" (Burgess, 2009: 309). Even if we accept the notion that security has no material form, security is by no means devoid of meaning. Security, as Burgess (2011: 2) has it, "embodies the social and cultural needs of a society, its hopes and fears, its past and its ambitions for the future." Security itself is a *value*, and as such it has been central to the history of political and social thought. Der Derian (1995: 25) even goes so far to claim that "within the concept of security lurks the entire history of western metaphysics", starting most prominently with Hobbes' (1651) mid-seventeenth century construct of the Leviathan as the foundation of society that can only exist through the fundamental basic desire for security. The Leviathan as a figure of thought embodies state sovereignty with the first and foremost task of putting an end to the war of everyone against everyone, such that mankind can escape its anarchic state of nature. As Huysmans (1998: 245) argues, "in the Hobbesian text security is a life strategy which manages uncertainty and ambivalence by producing truth and thus certainty and predictability." Thus, in the writing of Hobbes, security becomes framed as a constituting element of both power and of the state. The notion it carries, however, is a predominantly

positive, or, at best, a neutral one. This should remain so for quite some time. Indeed, as Neocleous (2008: 4) claims, throughout the main trajectories of classical political theory, "the common assumption remains that security is the foundation of freedom, democracy and the good society, and that the real question is how to improve the power of the state to 'secure' us."

Such a positive reading of security, however, in its core, is deeply rooted in rather isolated anthropological assumptions that do not adequately account for empirical contextualization. Its perspective on society is an external one, but it neglects the internal part. Subsequently, an overly positive notion of security has been fundamentally challenged throughout the twentieth century. As opposed to an abstract reading of security as something that has empowered the foundations of society early on, more contemporary engagements with security have sought to move beyond security as an isolated value, and engaged security as *part of society*. As Huysmans (1998: 228) argues, "the meaning of security does not just depend on the specific analytical questions it raises, it also articulates particular understandings of our relation to nature, other human beings and the self." Subsequently, the scope was re-calibrated to issues of how security actually plays out in the realm of the social. Thinking of security then becomes a normative premise and entails questions that are "concerned with the definition of the 'good' regarding security" (Browning and McDonald, 2013: 236), and subsequently with the 'good life' that security is set to protect (Ammicht Quinn, 2014). It is those very questions, however, that security constantly – and often incidentally – challenges through its very own mechanisms. Security, as de Lint and Virta (2004: 471) clearly put it, "produces the pathology it alone may cure." The effects of security thinking, of security politics, of security techniques and technologies, and of security practices carry a potential of backfiring at their creators such that they undermine other important values. In other words: security perpetually creates friction, and this friction can be felt and experienced in many registers of our everyday lives. As Martin and Simon (2008: 289) have it, security "is charged with preserving 'the way of life' or that which makes us insecure." Most prominent have been the recent debates on 'security vs. liberty' that had been reinforced in the post-9/11 era. The events of 9/11 should not be misunderstood as some kind of caesura, though, but rather as a catalyst that brought about a window of opportunity to legitimize and accelerate a plethora of minor and major security legislations, of tightened regulations and practices, and of technologies of surveillance and control.

Critical scholars have subsequently pointed out the detrimental effects of such a renewed desire for security on the social level: constant intrusions into spheres of privacy and intimacy, discrimination and social sorting, and, more generally, the undermining of a societal frame that was once outlined under the label of liberalism. As Bigo (2008a: 12) summarizes the critiques, security constantly runs the risk of becoming "disconnected from human, legal and social guarantees and protection of individuals." The oft-proposed image of a 'balance' or a 'trade-off' between security and other values such as fundamental rights or (civil) liberties, suggesting a more recent 'adjustment' of the relationship against the backdrop of terrorism and such, however, is a flawed one. First of all, in the vein of rather common critique, Hayes (2010: 158) claims that "in this 'trade-off' scenario, civil liberties and human rights have effectively been reduced to 'ethical concerns' that must be 'balanced' with the needs of security, and, by implication, can be restricted when the case for security has been made." It appears indeed a rather odd notion that some values could be diminished to the status of mere 'concerns', while others would remain untouchable. And second, as Waldron (2003: 193) argues, it starts from the questionable assumption that some optimal balance between the

two concepts could be struck in the first place. The very idea of a balance is an overly simplistic one, as it disregards the multiple (and competing) meanings of both security and liberty. Moreover, it disregards common objections to a purely consequentialist approach as well as questions of distributional justice and unintended (side) effects (Waldron, 2003: 195). It is precisely those questions that have become an integral part of a critical security studies agenda, and instrumental to the normative challenging of short-sighted security arguments. As Monahan (2006a: 21) points out, debates about 'trade-offs' or 'balances' "artificially constrain inquiry by offering little room to talk about deeper social changes underway." Security is not something to be treated lightly. Too many questions remain in between the Hobbesian notion of the founding principle of society and the contemporary notion that at times implies the status of a trump card. Questions of security must be inquired into with due care. After all, as Burgess (2011) notes, "we have come to understand that security comes with its own special ethical baggage."

One should thus be careful not to confuse the many different layers that security presents. Security is inextricably linked to forms of political and social organization, and as such connected to questions of power, authority and government. A lot of critique that at first sight seems to be directed at security itself, is in fact directed at a politico-economic agenda that operates under the paradigm of security. If, as Buzan et al. (1998: 4) claim, "security should not be thought of too easily as always a good thing", such an evaluation builds on its embeddedness on the political level. The distinction between the value of security and the political power of security, even if blurry, must thus always be kept in mind. A critique of security, as Neocleous (2008: 4) rightly points out, conceptualizes security "not as some kind of universal or transcendental value, but rather as a mode of governing, a political technology through which individuals, groups, classes, and, ultimately, modern capital is reshaped and reordered." Thus, as Burgess (2009: 310) adds, "the key to understanding security threats therefore lies in understanding the systems which link human values to the technologies that put them under threat." It is not so much the value of security itself that upsets and endangers societies, but rather its political transformations and social implementations. Those are the issues that I seek to explore throughout the ensuing narratives. After all, as Buzan and Hansen (2009: 26) remind us, "what is at stake in security debates is [..] often that empirical arguments and abstract ones challenge each other and this stacks the arguments in such a way that it is hard to find a resolution or even a common ground from which to debate."

First narrative: security as transformation[1]

The initial narrative has shown that security has been a driving force when it comes to the organization of the social, and subsequently the establishment of the political. But, as has also become apparent, the state-wielding security of Hobbes is not the security that Neocleous (2008: 5) rants against – the security that provides "the master narrative through which the state shapes our lives and imaginations (security risks here, security measures there, security police everywhere), producing and organising subjects in a way that is always already predisposed towards the exercise of violence in defence of the established order." Security as

[1] More precisely, this narrative should be entitled 'security *in* transformation', as it is deals with the (academic) transformation of security itself, rather than with the transformative potential of security. Although the title might appear a little misleading, I have kept it for the sake of coherence with the rest of the narratives.

such has always been subjected to *transformation*. This first actual narrative will engage with the changing notions of security that have become reflected in the way that academia has dealt with questions of security in the past (roughly) three decades. As Walters (2012: 2) has it, "that we live in times of profound transformation and uncertainty is, perhaps, something of a cliché" – however, there appears to be some truth in this oft-repeated mantra that becomes reflected in the evolving nature of security studies itself. The confusing multiplicity that we find in the academic landscape of security studies, broadly conceived, might be summarized such that security is very much a rapidly moving target. By asking a simple "Security! What do you mean?", Huysmans (1998) has programmatically summarized the debates around questions of means and actors, of reference objects, of scopes and limits, of fields and modalities, of threats, dangers and emergencies, of epistemologies and methodologies (Buzan and Hansen, 2009: 21).

While "security studies has been mixed up with strategic studies" (Bigo and Tsoukala, 2008b: 1) from early on and as such came into being as part of the classical IR agenda, the field has undergone major transformations that stand connected to a changing world (the end of the Cold War dichotomy, globalization processes, climate change, increasingly asymmetrical conflicts and ensuing migration movements, and many more), but also to new ways of thinking critically about security, and not least the incorporation of novel and multiple disciplinary perspectives (for instance, sociology, criminology, history, and law). As Lakoff (2006: 269) frames it, "to an observer a decade before, it might have been surprising that a natural disaster and a terrorist attack would be considered part of the same problematic." And yet here we are in a contemporary mode of security politics that desperately strive to cancel out every event that in some way could inflict harm on somebody (or something), and, in case this is not possible, at least be prepared to manage and mitigate disaster. And yet here we are in a contemporary field of security studies that has evolved throughout multiple layers of thought, that has challenged the conceptualizations of security over and over, and that has struggled to find a way to effectively bridge the gap between academia and 'real world security'. In short: the field of security studies now appears more dynamic, but also more fragmented than ever, and security discourses remain filled with contradictions in both epistemological and ontological terms. Whereas security was once framed as something that existed between sovereign nation states, and that could be counted in terms of military capacities (strength of standing armies, guns, tanks, and, most of all, nuclear weapons) and operationalized in positivist terms, its meaning over the last decades has substantially expanded in width and depth. As Lipschutz (1995: 8), paraphrasing Morgenthau, puts it, now "there are not only struggles over security among nations, but also struggles over security among notions." As such, new ways of thinking about security in a critical and multi-disciplinary fashion have also ascended to "refute the narrative of security as a 'branch' of International Relations" (Bigo and Tsoukala, 2008b: 6), and to pry away security studies from IR as its core discipline.

During the "interregnum" (Booth, 1991) of "soul-searching debates on widening and (sub)disciplinary identity" (Wæver and Buzan, 2007: 385) in the 1980s and 1990s, the general agenda of security studies arrived at a forking path. As Buzan et al. (1998: 2) argue, "the 'wide' versus 'narrow' debate grew out of dissatisfaction with the intense narrowing of the field of security studies imposed by the military and nuclear obsession of the Cold War." Subsequently, scholars started to open up the field for new and challenging currents such as peace research, post-structuralism, feminism, constructivism, human security, and post-colonialism (Buzan and Hansen, 2009: 187-8), thus "deepening the referent object beyond the state, widening the concept of security to include other sectors than the military, giving equal

emphasis to domestic and trans-border threats, and allowing for a transformation of the Realist, conflictual logic of international security" (Buzan and Hansen, 2009: 188). Particularly in Europe, scholars turned to the philosophical foundations of (security) thought and went on to challenge and transform the concept of security itself (Buzan and Hansen, 2009: 224).

On the other hand, scholars in the US stayed much closer to the original agenda. Some even uttered fears about the "risk of expanding 'security studies' excessively" (Walt, 1991: 213), which would, so the argument, ultimately undermine the intellectual coherence of the field and detach the academic agenda from the real world problems it was supposed to be concerned with. Particularly in the US, security debates remain predominantly framed around questions of power that derive from (neo)realist schools of thought, and that establish positivist narratives of causality in security politics. In what Wæver and Buzan (2007: 394) have identified as a rather pragmatic, problem-solving approach to security, analytics evolve not so much around the concept and meaning of security itself (and subsequently around its social implications), but around concrete approaches to concrete problems. Such a rationalist stance appears, in a sense, closely entangled in the core disciplinary roots of IR. Its analyses run along the lines of the nation state as the central actor in the international system, and as such paradigmatically enact Morgenthau's (1948) dictum of "politics among nations." Security, through this particular lens, then becomes predominantly framed as a matter of territorial integrity and the capacity to fight off enemy armies/military forces.

This is of course not to say that the ideal-typical US school of thought in security studies would not acknowledge the constant changes that our world is subjected to. On the contrary, with the events of 9/11 the latest, security scholars from all around the world have re-calibrated their foci – now zooming in on new forms of threat that come into being as "terrorist networks", "international crime", and such. Still, the positivist agenda of security studies is very much focused on foreign policy and warfare/armed conflicts. The European fork, on the other hand, has evolved in a particularly distinct direction. As Wæver (2004: 4) summarizes, there is now a vibrant debate of competing 'schools' in Europe, including the likes of critical security studies, the Copenhagen and Paris approaches to securitization theory, post-modernism, feminism, sociology of the international, and still almost 'classical' realist positions. Thriving on intellectual discourse rather than on analyses of the public level, security scholars went on to "reflect and problematize the concept – in order to understand and unveil the practices by practitioners in the name of security" (Wæver and Buzan, 2007: 394). There is, however, not much agreement on how exactly this should be done. Should the modality of security be constituted through threats, danger and corresponding exceptional states and measures, or rather through mundane practices and everyday bureaucratic routines (Hansen, 2008: 652)? As Buzan and Hansen (2009: 224) state, "there is, in other words, no one shared definition of what 'expanding security' should entail."

Where does this leave the current state of the art of studying security, then? There has not been one general trajectory, one straight path of flight that would have catapulted security studies beyond the intellectual challenge that was presented by the post-Cold War world. Rather, we find ourselves in an academic field that is struggling to find a common frame of identity. Against such struggle, I would, however, argue, that such an identity might not be necessary in the first place. The important lesson learned here is that the nature of security as such forbids a unified research agenda. Too manifold are its empirical manifestations, too manifold are its political applications, and too manifold are its ensuing social ordering processes to subsume them under one grand agenda. On the contrary, the ramifications of

security studies have had, after all, a positive effect. The toolbox of security studies has been substantially expanded and now provides a multiplicity of instruments that allow us not only to analyze, but also to challenge and critique security politics and practices. The latter is of utmost importance, if we keep in mind the initial narrative.

Thus, the picture that has been sketched out so far has introduced the fragmented nature of the academic field of studying security. A more or less common ground can be identified, however, in the acknowledgement that security problems have escaped the grip of the nation state. Be it the fact that terrorism is now framed as a global and border-crossing phenomenon, the insight that the 'classical', twentieth century warfare has been extinct for decades in favor of asymmetrical conflicts, or the awareness that all-encompassing threats such as climate change and resource scarcity cannot be resolved in national solo efforts. Modernity in its globalized fashion, simply put, has boiled down to the ontological blurring of the once distinct policy fields of external and internal security. What we find today, as Burgess (2009: 321) puts it, is a "growing de-differentiation between previously distinct activities: fighting wars abroad, controlling populations at home and managing the border between these two spheres." By any means, should the police or the army be responsive to cyber-attacks? And is a global pandemic an issue of maintaining internal order or one of fighting the disease abroad?

The diversification of both threats and the field of studying security have arguably evolved alongside each other. As internal security, traditionally concerned with crime fighting and policing, with civil protection and with the maintenance of (social) order, and external security, traditionally concerned with defending the territorial integrity of the state and possibly warfare (Eriksson and Rhinard, 2009: 245), started to converge, security issues demanded new ways of thinking in order to be analyzed, and the academic field of security studies did just that. Modernity has turned out to be complex and fast-travelling, and so have threats and, accordingly, security policies. As Eriksson and Rhinard (2009: 246) have it, "because modern security issues travel along systems that stretch across functional and geographical boundaries, 'transboundary security issues' offer prima facie evidence of at least some bridging of the internal-external security divide." The divide has become a nexus. As Bigo (2008a: 14) puts it, "we can no longer distinguish between an internal order reigning, thanks to the police, by holding the monopoly on legitimate violence, and an anarchic international order which is maintained by an equilibrium of national powers vis-à-vis the armies and diplomatic alliances." The transformation of security has in fact managed to transcend old-fashioned dichotomies, as today "it is not possible to draw a new boundary between internal and everyday politics on one side, and the international and exceptional politics also called security on the other side. The two are intertwined or more exactly related as if in a Möbius strip" (Bigo and Tsoukala, 2008b: 5).

Thus, what this narrative of security as transformation once more emphasizes is the fluidity of security. It undergoes constant challenges in both epistemological and ontological terms – and subsequently also in political and social terms. This leads to the next narrative: while scholars have long argued (and still continue to argue) how best to *think* about security, politicians are rather concerned about the ways in which to *enact* security. And while those two sides might not necessarily have a lot in common, they are yet unified by at least one question: what is the external condition that suggests, enables, imposes, and eventually *legitimizes* security? Or, put differently: how is security *reasoned*? This is what the ensuing narrative is about.

Second narrative: security as securitization

The first narrative has established the transformative notion of security that depends on the intellectual and political lens through which it is looked at. It has also introduced the rather limitless, constructivist notion of security as something that becomes defined by threats (which in terms also undergo constant transformation). Ultimately then, as Huysmans (2002: 42), paraphrasing Wendt, puts it: "security is what agents make of it." Thus, among such agents, security has entered a contested arena. Along the lines of this new way of thinking security, not only have concepts of security widened and deepened, but also has the theoretical toolbox of the discipline been substantially expanded. This second narrative looks into this toolbox. More specifically, it looks into securitization theory as a main theoretical framework that is concerned with how to analytically grasp the transformative processes that are induced by security *reasoning*. The seminal works of Wæver and his colleagues at the Copenhagen Peace Research Institute (now mostly referred to as the "Copenhagen school") established a frame of security as the construction of threat on the public and political level (Wæver, 1995; Buzan et al., 1998). They propose to look at security as "the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics" (Buzan et al., 1998: 23), eventually leading to *securitization* of areas/issues that had dealt with in the realm of regular politics before. Where threat in positivist theoretical stances was hitherto conceived of primarily as military capacities of states, this constructivist turn in security studies introduced an understanding of threats that emerge through discursive formations. As Buzan et al. (1998: 26) argue, "it is the utterance itself that is the act. By saying the words, something is done." Put simply: threats are *socially constructed* through speech acts – "threats have to be staged as existential threats to a referent object by a securitizing actor who thereby generates endorsement of emergency measures beyond rules that would otherwise bind" (Buzan et al., 1998: 5).

Such an utterance must not be misunderstood as a statement about the materiality of the threat itself, but in terms of the public and political perception of something as a threat. Through speech acts, any given risk (that might even be a part of everyday life, and that we pay no particular attention to) can be discursively lifted to the state of acute, existential threats that must be dealt with swiftly and decisively, since, so the argument goes, "if we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)" (Buzan et al., 1998: 24). This re-calibration of the analytical scope has considerably contributed to a re-conceptualization of security itself. Securitization theory is not so much interested in the nature of the threat, but in its transformation on the political level. By turning to the simple question of "what really makes something a security problem?" (Wæver, 1995: 54), the production of security against the backdrop of constructed threats emerges as the main scope for any analysis. Such a reading proposes an understanding of security that presents itself as flexible, fluid, and possibly all-encompassing, as it depends on the prevalent (political) discourse. In fact, as Guzzini (2011: 330) points out, in this vein "security is understood not through its substance but through its performance."

Framing something as a security issue then triggers a number of political consequences. Most notably it empowers the creation of an exceptional space where security threats can be tackled by the use of extraordinary means. Thus, the construction of threat on the political level transforms the political toolbox from what is at disposal in 'normal' politics to measures that would not be acceptable except for the state of emergency that had been induced by the

discursive framing of said threat. Notably, as will be dealt with in detail in the empirical section, the aviation system has been considerably securitized after 9/11, and against the backdrop of a presumed terrorist threat. As will be shown, new technologies, protocols, and modes of anticipatory governance have been implemented as a political response [Inquiries 1; 4; 6], bringing about major changes in how we experience security today [Inquiry 2]. To be quite concise here: for securitization theory, it is not so much the threat itself that is being constructed, but its *acknowledgement* as an existential security threat on the political agenda. Once such acknowledgement has been achieved, security politics exit the realm of democratic legitimization, and enter an exceptional void which is determined exclusively by the argument of bare survival. In the vein of Carl Schmitt (1922), exception must be defined as "a situation of radical danger and contingency for which no prior law, procedure or anticipated response is adequate. It is a perilous moment that exceeds the limits of precedent, knowledge, legislation and predictability" (c.a.s.e. collective, 2006: 465). Post-9/11 security politics have largely been analyzed as outcomes from such exceptional political spaces, having allowed for the implementation of laws and technologies that would not have been acceptable if not for the framing of terrorism as immediate and existential threat.

The notion of the exceptional has been contested, however. Especially when considering the extended duration of legislative processes and technological roll-outs and implementations, arguments that build on the immediacy to act *right now* appear rather unsuitable to hold up for multiple months or even years. And although several scholars have targeted the political attempts to permanently uphold states of threat and fear (Massumi, 2005; Bigo, 2002; Robin, 2004), others have pointed out the unlikely role of the exceptional as a driver in multi-level institutional processes (Neal, 2009). A second strand of securitization theory thus argues that it is processes of normality and routine, rather than discursively constructed states of exception, which play a major role in securitization. The so-called Paris school, which evolved around the works of Bigo and his colleagues (Bigo, 1994; Bigo, 2001; Bigo, 2002; Bigo and Tsoukala, 2008a; Bigo and Walker, 2007), thus pays attention to the professionals that manage and enact security on an everyday level. Through this layer, so the argument goes, "exceptional security practices can be understood in the context of ongoing processes of technocratic, bureaucratic and market-driven routinization and normalization" (c.a.s.e. collective, 2006: 466). Simply put, such an approach frames securitization as a long-term process that is not necessarily located on the political level, but that evolves through the administrative and practical layers, closely entangled with the economy and the development of new security technologies. Such a perspective will highlight the role of industrial stakes, research and development in the case of body scanners in [Inquiry 4]. Subsequently, discursive 'grand narratives' of security, as highlighted by the speech-act centered approach of the Copenhagen school, move to the background of the analytical picture. The main scope, on the contrary, lies on the underlying processes, rationalities, and practices of security. As Bigo (2002: 73) has it, "securitization works through everyday technologies, through the effects of power that are continuous rather than exceptional, through political struggles, and especially through institutional competition within the professional security field in which the most trivial interests are at stake."

The everyday, however, even though ontologically strongly opposed to the exception, does not imply a straight path of flight. On the contrary, as the c.a.s.e. collective (a collaborative project of, broadly conceived, critical security scholars, 2006: 456) points out, "normality is simultaneously a field of struggle, where technologies for constituting subjects and ordering the social come up against the intransigence of political agency and the resistance of political

subjects." Security, in this vein, remains contested, only that scholars inspired by the Paris school seek this contestation not on the public level of discourse, but rather in mundane activities and bureaucracies, in networks of experts and professionals, and in their claims that are underscored by the very expertise their occupation grants. As Balzacq (2011: 15) states, "the thrust of the argument is that beneath and above the 'discursive' level loom subtle yet decisive processes of securitization that only an approach through practices can disclose." Such a struggle for power entails claims of authority, which arguably at times gives practitioners an edge over politicians. They can rely on their field expertise when it comes to making a case for, or against, specific tools and technologies of security. The outcome of securitization processes, through this lens, remains very much open, and depends on a multiplicity of stakes. As Bigo (2002: 76) puts it, "the security process is thus the result of a field effect in which no actor can be the master of the game but in which everyone's knowledge and technological resources produce a hierarchy of threats."

In general, Paris school scholars start from the assumption that "practices of security are not given by nature but are the outcome of political acts by politicians and specialists on threat management" (Bigo, 2002: 68). Such a notion stems from the original focus on police work and police cooperation in Europe (Bigo, 1994; Bigo et al., 2007), as well as from the disciplinary roots of the Paris school that are located in political theory and sociology rather than in IR. Drawing particularly on the works of Bourdieu and Foucault, Bigo explicitly puts normative questions that derive from questions of security and its government on top of the research agenda. Mainly from research on EU migration policy and border control practices, he sketches out the dispositif of the ban-opticon, which is "characterized by the exceptionalism of power (rules of emergency and their tendency to become permanent), by the way it excludes certain groups in the name of their future potential behaviour (profiling) and by the way it normalized the non-excluded through its production of normative imperatives, the most important of which is free movement" (Bigo, 2008a: 32). Inclusion and exclusion, the permeability of borders and more generally the management of global flows of mobility in his analysis become closely entangled with the Foucauldian notion of a neoliberal agenda of letting productive elements (capital, goods, highly skilled and educated professionals) circulate while detaining those who cannot immediately contribute to the creation of economic surplus (asylum seekers, refugees, unskilled workforce).

Security analyses thus entail fundamental questions of human rights and civil liberties, especially when their violations fade into seemingly 'normal' bureaucratic routines, the invisible and irretraceable automated calculations of risk scores in large databases [Inquiry 6], or the permanent intrusions of privacy not only through physical means but through ubiquitous practices of data collection and storage [Inquiries 1; 3]. It is precisely this unspectacular level of ostensibly harmless and mundane measures that Huysmans (2011) has identified as "little security nothings." The by-default collection of credit card data, the retention of phone call details, or the CCTV camera on the street might not appear harmful. However, such nothings, when added up and used in the vein of a specific political agenda, can very much turn into security *somethings* that unfold the power to effectively (re-)order the social. The Paris school has made a strong case to look into those nothings/somethings through a sociologically informed methodology that is capable of probing the deeper levels of the emergence of security, and to subsequently drag them back to the light of the public, where harmful practices can be put under scrutiny and exposed to critique.

To even further complicate the intellectual configuration of securitization theory, a third 'school' has evolved in Aberystwyth, mainly through the works of Booth and Wyn Jones (Booth, 1991; 2005b; Wyn Jones, 2001). In the tradition of critical theory and thus predominantly aiming to challenge political notions of realism and positivism, scholars of this rather incoherent 'Welsh' variant of securitization theory highlight a vision of security that does not in any way oppress, but rather empowers individuals and thus unfolds an emancipatory potential – thus most notably "thinking about security from the perspective of those people(s) without power – those who have been traditionally silenced by prevailing structures" (Booth, 2005a: 14). As such, the normative aspects of Paris and Aberystwyth interpretations of security do not so much differ in their goals than in their intellectual foundations. Where the former builds on the works of Foucault and Bourdieu, the latter draws on Frankfurt School authors such as Adorno and Horkheimer.

The notion of schools, although compelling to structure the academic field, should however not be mistaken as a dogmatic distinction. In fact, as the c.a.s.e. collective (2006: 444) points out, "this categorization can be misleading if taken too seriously", as it would imply disconnected strands of thinking about security. While this is certainly true for the scope of the analytical levels and their respective methodologies, the normative core premises of Copenhagen, Paris and Aberystwyth scholars strike very much into the same direction. The 'abuse' of security as a means to enforce any political agenda, as opposed to the value of security as such, needs to be challenged – be this abuse constituted through the discursive construction of exceptional states of emergency, through incremental everyday practices and routines, or through the creeping power of the security industry, fostered by political means. This is ultimately the reason why Wæver (1995) initially called for the need to re-capture security and to re-establish it in the realm of regular, democratic politics: "desecuritization is the optimal long-range option, since it means not to have issues phrased as 'threats against which we have countermeasures' but to move them out of this threat-defense sequence and into the ordinary public sphere" (Buzan et al., 1998: 29).

If anything, the different strands of securitization theory can complement each other in order to close in on this normative goal. As Bigo (2002: 84) argues, "multiple discursive practices must be understood, as well as the heterogeneity of the nondiscursive practices as part of the same 'dispositif' (legal devices, political rhetoric, police practices, surveillance technologies, discourses on human rights, resistances of actors, and so on) in order to understand the articulation of knowledge and power relations." After all, security politics emerge through a "kaleidoscope of practices non-reducible to a core meaning or/and a linguistic formulation" (Balzacq et al., 2010), and which are not likely to be easily captured through one 'school' or another. Stritzel (2007) has thus argued to overcome the analytical fragmentation and aim for a holistic approach that incorporates the distinct theoretical advances and re-combines their strengths in terms of analytical levels and methodologies. After all, a more comprehensive theory of securitization must aim to interpret security and its capacities of power and knowledge both in "symbolic and institutional contexts" (Huysmans, 2002: 52), and possibly even beyond that. As the c.a.s.e. collective (2006: 451) summarizes, the aim must be "to go beyond the artificial boundaries in order to combine a variety of critical approaches under a common framework without, nonetheless, reducing one approach to another."

However, despite those attempts to mainstream the agenda of critical security studies, particularly the sociological approach of the Paris school has, at an early stage of critical scholarship on security, opened up an analytical agenda that moves beyond the 'classical'

inquiries of the international and national political levels, and threat-centered security reasoning. As Huysmans (2011: 375) puts it, "securitizing in contemporary world politics develops significantly through unspectacular processes of technologically driven surveillance, risk management and precautionary governance. These processes are less about declaring a territorialized enemy and threat of war than about dispersing techniques of administering uncertainty and 'mapping' dangers." This is what the next couple of narratives are about.

Third narrative: security as future

The third narrative explores a different strand of security politicality. If securitization is threat reasoning, then security epistemologies provide the underlying arguments for such reasoning. As is every other politics, security politics is concerned with the possibilities to actively shape the *future* according to a certain agenda or a particular (party) program, with the specificity that "for security policy, the assessment of dangers is essential" (Daase and Kessler, 2007: 415). However, unfortunately, the future (threat) can never be known until it eventually materializes. And yet politics are regularly evaluated retrospectively by their anticipatory performance. Faced with this dilemma, distinct attempts of getting a grip on the future have evolved in order to predict it and subsequently fold it back into the present where it can be rendered actionable and its outcomes can supposedly be modulated. Put simply, it is the very essence of any politics to extend its potential into the temporally unknown and by one means or another make it knowable such that political agency is created. As Anderson (2010a: 778) argues, "in the enactment of better worlds, the future is constantly being folded into the here and now; a desired future may act as a spur to action in the present." In security politics, subsequently, knowledge about threats must be created such that they can be tackled, and, in the best of worlds, canceled out, such that their detrimental impacts can be prevented. As Dillon (2011: 782) frames it, "the catastrophic threat-event of the dissolution of the temporal order of things is continuously also interrogated to supply the governing technologies, by which the political order is regulated in peace to be 'fit' for war and is regulated so as to resist the same catastrophic threat-event." It is the *event* that is rendered as the epitome of security futures, and that defines its governing technologies.

The event, in fact, is the great unifier of temporal uncertainties – the unifier under which all threats might be subsumed, no matter how dispersed their typologies might appear. As Lakoff (2006: 266) argues, a key mechanism for understanding security politics lies in the desire for anticipation and preparedness, for "in the imperative of preparedness, we find a shared sense of what 'security' problems involve today." The event is the ontological form of all that which in some fashion or another might disturb the state of security, and yet the acknowledgement of the event itself is an acknowledgement of the very impossibility of security. As soon as we speak of the event, its actualization, and subsequently the materialization of a security threat, is always already implied. The politicality of the event then hinges on the modes of addressing it, and arguably two major trajectories can be distinguished here. The first mode of security futures accepts the eventual actualization of the event, and subsequently turns to questions of disaster management in order to mitigate the *consequences* of the event. This opens up a wide array of actions. As Lakoff (2006: 267) has it, "preparedness is an 'abstract technology' that can be made concrete in diverse ways, according to different political aims." Preparedness can come into being through scenario planning, through simulation, or through the enactment of disaster and catastrophe. What those techniques have in common is the

creation of practical experience that can act as a guideline for behavior in similar (or different) contingencies.

The second mode of addressing the future is to actively intervene into contingency and to try to *cancel out* the event. Even though especially post-9/11 security politics have emphasized such a need, both modes are not by any means mutually exclusive. On the contrary, they can be found throughout contemporary security policies in a multiplicity of empirical forms and combinations. What both temporally divided modes have in common is an epistemological quest – a quest for knowledge about the future, that is. As indicated above, there can be no certainty about the future, but only the twisted notion of certainty about the radical contingency of life. And yet, security politics must strive to come to actionable terms with this basic human condition of being incarcerated in the present. As Daase and Kessler (2007: 419) argue, "dangers are always conceptualized in terms of a 'lack' of knowledge. Dangers manifest themselves owing to incomplete knowledge." As soon as the future could be rendered knowledgeable, so the best world scenario goes, it could be unlimitedly modified, and hence, *secured*. The lack of actionable foresight has been subjected to countless political and academic debates, and has been considerably re-kindled by the event of 9/11. The main trajectory of political discourse in its aftermath was that the attacks should have been thwarted by the US intelligence services – and that they could have been thwarted if only the available dots had been connected and thus rendered actionable in advance. Scholars have since been increasingly concerned with analyses of the evolving political ways of doing just that.

The political twist of security, thought of in temporal terms, is to find a suitable mode of addressing the future in order to be able to reason about security in the future. However, due to the contingency that defines our existence in the world, extending knowledges beyond knowledge can never render any claims about futures to be *true*. As Dillon (2011: 782) argues, "every politics of security, by virtue of the very fact is a politics of the limit", but there is a regular exceeding beyond such limits that is reflected in contemporary security politics. While being epistemologically virtual, security creates material impact. Instead of speaking epistemological truth, security (politics) has found a multiplicity of distinct ways to break down, rationalize, and calculate the future. Arguably, the most crucial and widely acknowledged mode of addressing the future is through the modality of *risk*.

As Beck (2002: 40) has prominently laid out, risk represents an epistemologically impossible attempt of capturing contingency under the umbrella of rationality: "as soon as we speak in terms of 'risk', we are talking about calculating the incalculable, colonizing the future." Subsequently, such an effort to calculate what cannot be calculated would ultimately result in the insight that through risk we merely might "feign control over the uncontrollable" (Beck, 2002: 41) – without ever actually controlling it. Despite those epistemological shortcomings, numerous scholars have shown how a risk calculus is nonetheless politically applied in the domain of security (Aradau and van Munster, 2007; Daase and Kessler, 2007; de Goede and Randalls, 2009; Amoore, 2011; Lobo-Guerrero, 2011; Amoore and de Goede, 2008b). Risk, politically speaking, is then not necessarily a means of knowledge creation, but a means of government. Security becomes *governed through* risk (Aradau and van Munster, 2007), a notion that is taken up by [Inquiries 1; 6].

This notion of risk as technique of government is very much reflected in its genealogy. Ewald (2002: 283), in his analysis of the evolution of risk, notes that "we are now re-discovering the existence of disaster, but with the difference that disasters are no longer, as before, attributed

to God and Providence, but to human agency." Risk, by capturing contingency and folding it into human agency, rationalizes what was once left to the supernatural, and translates destiny into modifiable and manageable numbers. The logic of probability is born out of modernity's attempt to create ultimate control over the world. As Daase and Kessler (2007: 417) explain, "the emergence of probability, in other words, parallels an overall transformation of societies manifested in the discovery of the subject, social contract theory, the invention of positive law and subjective rights, and thus a particular modern notion of knowledge and understanding of how the world might be known." The overarching notion here is one of humanity actively striving to get in control of itself and its surroundings. Rationalization and governing are intertwined concepts, with risk providing a capable connector to both create an account of the world and to subsequently mold it.

The concept of risk has been subjected to multiple political and social transformations throughout modernity. Ewald (2002) identifies a series of shifting notions, ranging from providence to prevention and eventually precaution, thereby tracking the incorporation of risk from the individual to the societal level and its evolving openness to the exceeding of 'hard' science. While risk as providence is still "linked to the notions of fate, chance and misfortune, and hazard" (Ewald, 2002: 293), prevention for the first time seeks to establish calculability and as such a "rational approach to an evil that science can objectify and measure" (Ewald, 2002: 293). It is this very extrapolation from measurement and past experience that Beck has criticized as epistemologically pretentious – but nonetheless politically powerful. However, in this vein, as experience has time and time again demonstrated the factual impossibility to calculate the future, another mode of risk has emerged. Precaution strives to supersede the notion of statistics by addressing "threats and dangers that are irregular, incalculable, and, in important ways, unpredictable" (de Goede, 2011: 9). Most prominently, Beck (1999) has shown how the "precautionary principle" has emerged through the uncertainties of environmental damage and the attempts to get a grip on its possible consequences. As such, "precautionary logics act before the identified threat reaches a point of irreversibility" (Anderson, 2010a: 789), thereby diving deep into the realm of future scenarios that are not necessarily grounded in facts.

Anderson (2010a), in his analysis of the event, adds preemption as another layer of risky futurity, exceeding the previous. Preemption has come to enact a prominent role in the so-called 'war on terror', as it accepts the fact that future events cannot by any means be known in their eventual shape, and might thus considerably differ from known events of the past. This insight has been (in)famously expressed by former US Secretary of Defense, Donald Rumsfeld, when he referred to the "unknown unknowns" that security faces in the proclaimed 'war on terror'. Preemption strongly overlaps with precaution, in which, as Amoore and de Goede (2008a: 11) frame it, "a desire for zero risk joins a vision of worst case scenarios in order to enable preemptive action against perceived terrorist threats." However, as Anderson (2010a: 790) argues, preemption has to "break with the logic of risk", as it "acts over threats that have not yet emerged as determinate threats."

In this vein, preemption appears as epistemologically puzzling, as it seeks to produce security against the backdrop of a double uncertainty. Neither do we know, according to its logic, *what* the event will be, nor do we know *when* it will occur. Due to the epistemological break with the rationality of risk, preemption strives to render the event knowable in different ways. As Massumi (2007) has argued, preemption operates in a virtual realm of potentialities that are folded back into the actionable real world without ever realizing their potential – therefore

endlessly circulating and eventually leading to what Amoore (2013) has compellingly described as a "politics of possibility." Partly being grounded in the same efforts of data collection and modelling as risk calculus, but at the same time aware of the fact that the probability rationale can never suffice, preemption then opts to operate at the interstice between real world facts and the virtual possibilities that can be derived from them. [Inquiry 6] looks into such practices empirically, building on proposed advanced analytics of PNR data in order to establish new types of threat hypotheses – and the potentially devastating consequences for the legal anti-discrimination framework. As a probability calculus inevitably fails in the face of the unknown, preemption strives to incorporate possibility and has thus in fact ascended to be the new and more fitted mode of political action (and reason).

The failure of traditional modes of anticipation has been broadly made evident by 9/11. The event itself had obviously superseded the anticipatory capacities of US security agencies, as it had not been subjected to sufficient action to prevent it. In fact, as the report of the 9/11 Commission (2004: 343) points out, "there was uncertainty among senior officials about whether this was just a new and especially venomous version of the ordinary terrorist threat America had lived with for decades, or was radically new, posing a threat beyond any yet experienced." It is precisely this distinction from past experiences that had disabled modes of probability calculus – the logics of security appeared to remain stuck in well-known patterns of threat and failed to engage the openness and creativity of the terrorist cell that eventually turned out to cause the catastrophic event. Despite recognizing that hindsight is always 20/20, the report goes on to state that, "looking back, we are struck with the narrow and unimaginative menu of options for action offered to both President Clinton and President Bush" (9/11 Commission, 2004: 350). If it was indeed a failure of imagination that had undermined security operations that could have prevented such a devastating event, then how to prevent this failure in the future? How to get a better grip of the future?

Academic debates have been rather cautious about those questions. As Daase and Kessler (2007: 427) argue, "to the extent to which terrorist attacks are perceived as a disaster in the sense of the *unknown unknowns*, the FBI and the secret services of the world are off the hook, as the possibility of 'governing', regulating and taming terrorism diminishes [emph. in orig.]." Radically speaking, security epistemologies can only ever be a mere approximation of the future. Indeed, if there is "a clear connection between the concept of security and epistemology" (Buzan and Hansen, 2009: 32), then it must ultimately epitomize in the impossibility of a definite temporal epistemology of security.

Politicalities of the future, however, need not necessarily come to logical terms with their epistemological pitfalls and fine-grained modalities. As O'Malley (2000: 459) summarizes the rather simple mechanism of anticipatory security politics: "risk is imagined, both by the governors who deploy it, and by those who study its deployment, as an element in the conduct of conduct." Thus, politically, the modes of addressing the future serve as a means of (re-)ordering the social. It does so through governing techniques that build on and are embedded in the rationalization processes of modernity that introduced risk in the first place. As Anderson (2010a: 784) argues, "the result is that specific futures are made present through the domain of number, numbers which are then visualized in forms of 'mechanical objectivity' such as tables, charts and graphs." However, if specific futures are made present, then on the flipside other futures are rendered invisible by modes of non-representation, and this is the very mechanism that Daase and Kessler (2007: 428) identify as the point of entry for a political

and social agenda, as "not-to-be-wanted-to-be-known knowledge is systematically withheld or disregarded as soon as it does not fit with operative concepts."

The representation of futures easily exceeds the logics of statistical models as soon as, as Amoore (2011: 27) frames it, "contemporary risk calculus does not seek a causal relationship between items of data, but works instead on and through the relation itself." Such an operation becomes even more problematic, as "risk calculation itself is never made visible" (Amoore and de Goede, 2008a: 6) and thus re-locates security into the realm of the opaque that cannot be retraced, challenged or critiqued (Rouvroy, 2013). As Amoore (2011: 30) argues, "there can be no certainty about the association between data on a flight route, a method of payment, ticket type, or a past 'no show', for their relation is not causal but correlative. What matters instead is the capacity to make inferences across the data, such that derivatives can be recognized, shared, and actioned." Security as future is not constructed as an argument based on facts, but rather as an argument based on speculations – and if speculations introduce an element of suspicion which must necessarily canceled out by intense scrutiny on all levels, then the epistemological rifts of the future pan out in the present [Inquiries 1; 6].

Subsequently, there are major implications from the transformation of risk as a mode of governing. As Bigo (2008b: 113) explains, "if security is a governmentality of risk and risk is now associated with a worst-case scenario beyond any calculus of probability and a quasi-astrological assessment of the future, then any contingency read as an accident, a major catastrophe, a possible Armageddon, re-enacts the argument of the exception inside the risk approach." Here the narrative of security as future re-connects to the narrative of security as securitization. Futures produce virtual emergencies that could materialize at any given moment. If, as Daase and Kessler (2007: 418) argue, "risk names the boundary of what an individual can and does (not) know, what lies in his responsibility or what is subject to, for example, a 'higher force'", then the modulation of risk itself on the political level creates an effective mechanism that not only enables knowledges, but at the same time disables other knowledges – knowledges that arguably conceptualize security futures as ordinary futures that need not rely on exceptional political states.

As has been shown earlier, threats create spaces of ultimate political agency, even if their status remains forever virtual. Managing such virtuality then becomes key for any politics of security, as the nature of virtuality defines what is governable. If "risk-based calculative models and practices are emerging as a key means of identifying vulnerable spaces and suspicious populations in the war on terror" (Amoore and de Goede, 2008a), then who controls the nature of risk can subsequently claim control over both spaces and populations. As Amoore (2005: 149) puts it, "from the protection of borders to international financial flows, from airport security to daily financial transactions, risk assessment is emerging as the most important way in which terrorist danger is made measurable and manageable." The individual then becomes recoded into a possibly disruptive element whose detrimental potential must be canceled out or neutralized. This brings about major implications for any critique of security and its modes of analysis. As Bigo (2012: 283) points out, from a normative standpoint "it is then central to analyze the transformation of democracy and freedom implied by a view of the future as a future already known, as a 'future antérieur', as a future perfect."

Scholars have indeed been increasingly concerned with the consequences that emerge from such a fetish of the future, most notably in terms of social sorting and discrimination, but also in terms of the legal framework. As Tsoukala (2010: 44) argues, "vanishing legal personhood

is not a side effect but the natural outcome of the prevalence of the risk-focused mindset in both the crime control and the human rights realms." Attempts to theoretically re-capture an enforceable legal status appear in fact rather bleak. This is partly due to the ubiquitous and invisible nature of contemporary data surveillance that has become a key element of the government through risk. As Bigo (2008b: 109) claims, "by dematerialising through data information-gathering, a security dispositif not only acquires a speed that transcends borders, but also an ambition to monitor and control the future through profiling and morphing." We will in greater length come back to such issues in the fifth narrative that looks into security as surveillance. Another consequence from security as futurity is the increasing detachment from democratic mechanisms. As Aradau and van Munster (2007: 108) have it, "the infinity of risk does not lead to a democratic politics that debates what is to be done, but to intensified efforts and technological inventions on the part of the risk managers to adjust existing risk technologies or to supplement them." This second strand of implications will be further tackled in the sixth narrative that deals with security as technology.

Fourth narrative: security as government

The preceding narrative has already laid out some of the analytical issues that are to follow. However, before turning to the narratives of security as surveillance and technology, this fourth narrative explores the seemingly banal notion of security as government. Given its political and social registers, it would indeed be a contradiction in terms to speak of security *not* as government. In this vein, all of the empirical inquiries of this thesis are concerned with security as government. However, what at first glance appears as a rather basic insight in fact opens up a wide agenda for research on specific governing techniques that build on security as their core preoccupation. As Dean (2006: 22) puts it, "an analytics of government takes as its central concern *how* we govern and are governed within different regimes, and the conditions under which such regimes emerge, continue to operate, and are transformed [emph. in orig.]." In order to come to terms with such analytics, we must distinguish between two major strands of literature that are concerned with the government of security. Research on *security governance* has been predominantly concerned with the changing role of the state and private actors in policing and the provision of security within national boundaries more generally. The second body of literature is rather concerned with the notion of governing itself, and explores how it plays out through complex assemblages and controversies, and how distinct techniques of governing have historically been evolving around particular problematiaztions. Such a notion of *governmentality* is deeply rooted in the works of Foucault, and has more recently been valued and taken up by scholars of security.

Foucault has plainly framed the central issue of concern for any analysis of government around the question of how power can be exercised over individuals and populations such that their behavior can be modulated. "Governmentality, that is to say, the way in which one conducts the conduct of men" (Foucault, 2008: 186), must be understood as historically contingent and emergent, however not bound by some underlying trajectory or political *telos*, but rather as the resultant from temporally and spatially specific problem constellations. To think about government in terms of governmentality requires us to move away from state-centric conceptualizations, and even from the general notion of the possibility of centralized power that could be executed by a single instance according to a specific rationality. Traditionally, as Dean (2006: 9) points out, "in most cases the question of government is identified with the state", but such a conceptualization of government in fact falls short of how government

comes into being empirically. Instead, an acknowledgment of the multitude of forces that consistently negotiate and re-negotiate political programs, concrete policies, and fine-grained, capillary sets of practices then frees any analysis of government from the risk of reproducing simplistic binaries of state power/population submission. For Foucault, power is not something can be identified and pinned down in one particular location. Rather, power is relational and as such something that is constantly produced and re-produced among multiple agencies and actors. As Dean (2006: 29) puts it, "power, from this point of view, is not a zero-sum game played within an *a priori* structural distribution. It is rather the (mobile and open) resultant of the loose and changing assemblage of governmental techniques, practices and rationalities [emph. in orig.]."

Thus, we must not look for power, and subsequently government, exclusively in the domain of the state. As Foucault (2008: 6) emphasizes, "the state is not a cold monster; it is the correlative of a particular way of governing", incorporating a multiplicity of elements and techniques. Thus, if "all organised social existence, including all practices of liberty, presupposes forms of the 'conduct of conduct'" (Dean, 2006: 35), then how can we analytically come to terms with such conduct of conduct? In order to do so, we must return to the question of power and its re-conceptualization from a technique of domination to a capillary and free-floating construct devoid of any presupposed agenda. As Walters (2012: 14) explains, "within the nominalist worldview that Foucault cultivated there is no power in general, only specific 'dispositions, manoeuvres, tactics, techniques, functionings' that it is the researcher's task to carefully map, and distinguish." It is in fact an empirical research agenda that must derived from such an understanding of government.

Foucault has in his works genealogically centered around the emergence of historical techniques of government, understood in the form of 'events' such as the "birth of the prison" (Foucault, 1977), the "birth of the clinic" (Foucault, 1994), or the "birth of biopolitics" (Foucault, 2008). The historical scope as well as its radical empiricism have rendered the notion of governmentality as "highly capable of registering all manner of subtle (and not so subtle) shifts in the rationalities, technologies, strategies and identities of governance" (Walters, 2012: 3). Governmentality, as Walters (2012: 18) has it, must indeed be interpreted as a call to "engage all objects – and subjects – as effects, as products, as entities that are not natural but as emergent within contingent historical processes", and thus to provide an account of power and government as precise as possible.

Thus, how has the government *of* security, and, most notably, *through* security, been analyzed empirically? As has been indicated above, a wide body of literature on security *governance* has evolved mainly through the works of criminologists and scholars of (penal) law, taking off in the 1980s. In the fashion of the Foucauldian scope on historical events, we might think of the preoccupation of this literature on private security as 'the birth of commodification', as it centers around transformations of police work and the increasing role of a growing security market. It is arguably this scope on the market that has led to the fact that "in a great deal of the literature govermentality has been used and interpreted as almost synonymous with *liberal* and/or *neoliberal* governance" (Walters, 2012: 10). As Wood and Dupont (2006b: 2) clarify with regard to the criminological notion of security governance, "the term 'governance' in this context refers to conscious attempts to shape and influence the conduct of individuals, groups and wide populations in furtherance of a particular objective – in this case, 'security'." Be it framed as governmentality or as governance, what unites both strands of research is their reluctance to ascribe a prioritized role to the state. Research on security governance has

been preoccupied with the transformation of police work and thus with specific constellations of 'internal security' that have become shaped by processes of rationalization and privatization. Subsequently, we can find a strong economic notion in these works.

Thus, how did such a presupposed 'birth of commodification' come about? How come the provision of security through state agencies today at times appears to be equated, if not superseded by private security companies (and analogously the military by private military companies)? As Jones and Newburn (2002: 134) point out, "current developments are perhaps [..] better presented as the continuation of a long-term trend extending back several decades rather than a seismic shift occurring in the dying years of the twentieth century." We might even have to go further back. As Marquis (2003: 231) highlights, "private policing, far from being a twentieth-century invention, was a creature of the Commercial and Industrial Revolutions" and as such must be conceived as a contingent phenomenon that has evolved alongside the emergence of increasing wealth and private property that had to be protected – but recently also with a fundamental shift in penal law that has profoundly affected policing practices. As Feeley and Simon (1992: 452) argue, this "new penology is markedly less concerned with responsibility, fault, moral sensibility, diagnosis, or intervention and treatment of the individual offender." Those classical paradigms of prosecution and punishment have been partly abandoned and re-combined with new elements that have arrived in the wake of liberal developments and privatizations, most prominently in the US and the UK. A resulting new mode of penal law, as Feeley and Simon (1992: 452) have it, is then "concerned with techniques to identify, classify, and manage groupings sorted by dangerousness." In other words, policing has been transformed into a managerial task that engages the future on the basis of risk.

Such a mode of security provision strongly re-connects to the preceding narrative of security as future that has explored the notion of risk more in-depth. Ericson and Haggerty (1997) have compellingly shown how policing has been re-constituted through the paradigm of risk. As Ericson (1994: 151) frames the central issue, the preoccupation for the police has adjusted according to such a logic of risk – now "it is knowledge for security that constitutes their trade." If police work is mainly knowledge work, then subsequently the task of actually enacting security on the ground level must not necessarily remain within the domain of the police, after all. Security, through such transformation, has become a tradable asset and its provision is "becoming ever more fragmented and commodified" (Loader, 1997: 377). This is not to say that state security forces would have withdrawn from their classical tasks, but that the emergence of a 'market' for security has created a multiplicity of constellations – including the outsourcing or out-contracting of policing to private security firms, public-private partnerships, and the establishment of novel security provisions such as the patrolling of a specific neighborhood by private companies that had not been covered by the state before – that subsequently have brought about a multiplicity of questions towards the normative implications of such new assemblages of security. [Inquiry 5] engages such new constellations empirically, looking into practices of out-contracting screening duties at German airports.

Speaking in very simple terms, "governance can be good or bad" (Rose, 1999: 16), and along this simple question the literature is indeed very much divided. While some have argued that "*new* and *re-configured* forms of community governance can serve to address, and ideally reduce, the governance deficits [emph. in orig.]" (Shearing and Wood, 2003a: 207) that have been diagnosed as inherent to an inflexible apparatus of state agencies, others have uttered considerable doubts towards the very idea of a commodification of security provision.

Referring to security as value, as has been laid out in the first narrative, Loader (1997: 383) highlights that "there is something about security that means its provision cannot simply be left to the unfettered market." From such a perspective, security as government then must be strongly linked to the state due to issues of accountability and democratic legitimization of the execution of power through state agencies. In this vein, only the state, as represented through the police and other state agencies, would be legitimized to provide and enforce security. From a normative stance, as the c.a.s.e. collective (2006: 464) summarizes, "the aim, here, is to understand what happens when discourses of (in)security, historically considered as enactments of state sovereignty, are said to refer to the presumably 'marketized' and 'democratized' realm of private security operators."

In fact, as Loader (1999: 386) argues, there is a "diffuse unease about permitting market imperatives to determine the distribution and accountability of policing and security." Such unease arguably derives from the increasingly neoliberal colonization of security as a market in the first place, and the ensuing reluctance to establish clear-cut regulatory boundaries for something as delicate as security (Zedner, 2006a: 276). After all, from a neoliberal perspective, such mechanisms would hurt the market equilibrium, and subsequently decrease its efficiency as well as the profits that can be generated through the provision of security. The seventh narrative of security as economy will engage with issues of marketization and privatization of security in more depth. For now, we must keep in mind that research on the transformation of policing has relatively early come to terms with the empirical notion that "on a continuum of a whole range of commercial services, it is now increasingly difficult to say where the private security sector begins or ends" (Jones and Newburn, 1996: 106).

The messiness of such a continuum approach is the very notion that re-connects research on security governance to scholarship on the broader notion of governmentality. As has been empirically diagnosed within the field of policing, in governing processes "there is a plurality of governing agencies and authorities, of aspects of behaviour to be governed, of norms invoked, of purposes sought, and of effects, outcomes and consequences" (Dean, 2006: 10). Security as government then must necessarily be thought of as something that needs to be empirically researched in order to understand its elements and the involved stakes, trajectories, actors, institutions, and the problems around which they constitute themselves. As Rose (1999: 18) summarizes the task, such research includes "the invention and assembly of a whole array of technologies that connected up calculations and strategies developed in political centres to those thousands of spatially scattered points where the constitutional, fiscal, organizational and judicial powers of the state connect with endeavours to manage economic life, the health and habits of the population, the civility of the masses and so forth." The analysis of such scattered and dispersed elements then needs to be realized through the opening up of assemblages of government, through their careful disassembly, and through scrutiny of the discourses that have rendered them powerful against the backdrop of particular (security) problems of government.

In such disassembly lies powerful critical potential. As Dean (2006: 38) emphasizes, "an analytics of government removes the 'naturalness' and 'taken-for-granted' character of how things are done" and thus opens up the possibility to question the particular nature of assemblages of security. Why is security structured the way it is? Why have surveillance, technologies, and the economy evolved as such strong leitmotifs of security, as will be laid out in the following narratives? As Rose (1999: 18) has it, "it is within this field of governmentality that one sees the continual attempts to define and redefine which aspects of government are

within the competence of the state and which are not, what is and what is not political, what is public and what is private, and so forth." Thus, an analysis in the vein of governmentality can not only help to diagnose the modes in which government is enacted through the domain of security, but at the same time expose and challenge them. Such challenge must then run through the registers of truth and knowledge that are constitutive of the power that enables the conduct of conduct. Neither of those categories are stable, however. Regimes of government "involve practices for the production of truth and knowledge, comprise multiple forms of practical, technical and calculative rationality, and are subject to programmes for their reform" (Dean, 2006: 18-9).

Such continuous reform is in fact crucial for an analysis of security as government. As Dean (2006: 27) points out, "the key starting point of an analytics of government is the identification and examination of specific situations in which the activity of governing comes to be called into question, the moments and the situations in which government becomes a problem." Government that evolves through security, as has been shown, must build on the construction and/or acknowledgement of specific threats. Most strikingly, for a large part of more than one decade by now, security politics have been dominated by the paradigm of global terrorism, and governing practices in the name of counter-terrorism have, based on the argument that terrorist attacks could happen anywhere and at any time, extended deeply into our everyday lives. The problems/threats to be governed are not limited to issues of terrorism, however. As has been shown earlier, security threats are rather limitless in their nature and can come into being through various layers of discourse, practices, knowledges, and technologies. Nonetheless, around such problematizations of security in the form of threats evolves the politicality of security, and thus in the Foucauldian conceptualization they must be researched as contingent events of shifting modes of governing. As Rose (1999: 19) frames the issue, governmentality presupposes "studies of a particular 'stratum' of knowing and acting. Of the emergence of particular 'regimes of truth' concerning the conduct of conduct, ways of speaking truth, persons authorized to speak truths, ways of enacting truths and the costs of so doing. Of the invention and assemblage of particular apparatuses and devices for exercising power and intervening upon particular problems."

In terms of the specific field of security then, as Dupont (2006: 87) lays out, "the multiplication of institutional actors and corporatist interests that seek to maintain or enhance their position has created many sources of frictions and opportunities for power struggles, over or covert." Taking into account those very struggles then indeed opens up a space for normative intervention, as it enables an "open and critical relation to strategies for governing, attentive to their presuppositions, their assumptions, their exclusions, their naiveties and their knaveries, their regimes of vision and their spots of blindness" (Rose, 1999: 19). In summary, analyzing security as governmentality implies the willingness of the researcher to fully cherish the messy and complicated nature of government and to analytically, as well as normatively, thrive on the radical insight that things could have turned out different, thus in fact empowering distinct (virtual) conceptualizations of security.

Numerous scholars have built on such a contingent notion and have used such spaces in order to put forward blazing critique towards contemporary regimes of security that at times appear to be dominated by an emphasis on threat and insecurity. Indeed, a common frame of such critiques is a reading of government through *insecurity*. As Neocleous (2008: 4) provocatively asks, "what if at the heart of the logic of security lies not a vision of freedom or emancipation, but a means of modelling the whole of human society around a particular vision of order?"

Arguably, we must keep in mind here the fact that security always prescribes its own pathology. As the c.a.s.e. collective (2006: 460) points out, this pathology entails a security trap, meaning that "one cannot necessarily establish a feeling of security, understood as a feeling of freedom from threat, simply by securitizing more issues or by securitizing them more." As Balzacq (2011: 2) argues, "in short, security problems can be designed or they can emerge out of different practices, whose initial aim (if they ever had) was not in fact to create a security problem." But what if this pathology was to be used and modulated by contemporary modes of government as a means of exercising power according to specific aims? As Bigo (2008b: 105) argues, "security produces insecurity. It excludes in the name of protection and always discriminates within society. It abnormalises the margins and creates boundaries within the social space." The ensuing narrative explores how such a presupposed agenda of social sorting comes into being through security as surveillance.

Fifth narrative: security as surveillance

The fourth narrative has explored security as a technique of governing, both through the complex and contingent modes of its production, and its positioning alongside the continuum of the public-private divide between both state and non-state actors. Following up on this notion, the fifth narratives engages a particular technique of governing that is not exclusively limited to contexts of security, but that has nonetheless become inextricably linked to discourses of security: surveillance. Surveillance is not by any means a phenomenon of the digital age (Marquis, 2003: 226), but, as Monahan (2006a: 10) argues, "even before the automation of surveillance, modern bureaucracies and architectures functioned as pervasive technical systems of social control." However, as Lyon (2003b: 1) notes, surveillance "now occurs routinely, locally and globally, as an unavoidable feature of everyday life in contemporary societies", rendering it part of the array of mundane and often unnoticed practices that are crucial for any sociologically inspired analysis of securitization processes. Physical surveillance (most notably the human gaze and its electronic successor, CCTV) today has long been surpassed by digital surveillance, or, as Amoore and de Goede (2005) have framed it, "dataveillance."

In the data-driven and digitized environment we face today, data are almost by default harvested as we carry out everyday tasks such as making phone calls and writing e-mails, surfing the internet and shopping by credit card, or in fact just walking the streets. This has indeed led to a widely acknowledged notion of quasi-limitless surveillance. Subsequently, in their seminal article on the state of surveillance in contemporary societies, Haggerty and Ericson (2000: 611) have migrated Rousseau's dictum of the impossibility of freedom to a rather bleak description of present times' dataveillance. As they have it, "humans are born free, and are immediately electronically monitored." Surveillance, as Lyon et al. (2012: 1) argue, enacts a social ordering process that "comprises the collection, usually (but not always) followed by analysis and application of information within a given domain of social, environmental, economic or political governance." Any research agenda centered around surveillance must thus focus on what happens with data. How are data collected, stored, transformed, combined, circulated, and eventually algorithmically analyzed in order to create power and control? After all, "categorizing others necessarily contributes to how we treat them" (Jenkins, 2012: 160) and thus entails a multitude of political and social implications.

As Ball and Webster (2003: 7-8) point out, distinct domains of application in fact foster different types of surveillance, ranging from the seduction of customers based on

consumption profiles, to the categorical exposure of personal details in the media, and eventually to proposed beneficial forms of surveillance for the purpose of improved services and care in the health sector. Especially the latter has become a fashionable argument lately, as it arguably depicts a benevolent form of surveillance that one can hardly be opposed to. However, as Monahan (2010: 91) warns, "although control could be exercised with surveillance systems for purposes of care or protection, such systems are most often characterized by coercion and repression, and offer few avenues for accountability or oversight." With regard to health care, for instance, insurances have shown strong interest in the medical records of patients in order to improve their risk assessment models and adjust payment rates for given individuals. Thus, if diagnostic data of some kind of disease would leak from medical records, insurance rates in that scenario would quickly sky-rocket. Benevolence would then quickly be turned into a ruthless business case – with both angles hinging on the power that surveillance creates.

Of most relevance for questions of security, however, is the categorical suspicion that "involves surveillance that is concerned with identification of threats to law and order" (Ball and Webster, 2003: 7). In this vein, as Bigo (2008a: 18) adds, "surveillance projects itself on spaces, states, and persons seen as a danger and a threat to national security and public order." Thus, surveillance is a highly effective technique for ordering the social. As Murakami Wood et al. (2003: 150) argue, the all-encompassing nature of scrutiny possibly enabled by surveillance practices relies on a very simple mechanism of power imbalance between the 'watcher' and the 'watched' that must be closely scrutinized in its empirical forms. Ultimately, as they frame the issue, "surveillance is a uniquely simple concept, but is an empirically complex, emergent phenomenon, and is inextricably bound up with issues of power." Analyses of such issues of power imbalance often draw on Bentham's (1995) prominent figure of the panopticon. The panopticon, an architectural design for a prison originally published in 1787, would allow prison guards to visually survey all areas of the building from a centralized room. The prison inmates, on the other hand, would not be able to see the guards, rendering the panopticon an effective mechanism of control.

Foucault (1977) has later taken up the figure of the panopticon, but analytically from a reverse angle. Whereas for Bentham, the idea of prison surveillance was linked to a very concrete empowerment of guards and his subsequent argument about improved effectiveness of control mechanisms, the Foucauldian angle rather highlights the effects of such surveillance on the prisoners. For Foucault, the panopticon enacts a power asymmetry between the watchers and the watched, most notably disciplining the latter by implying the mere possibility of being watched at any given moment. As Elmer (2012: 23) explains, "Foucault's panopticon emphasizes an enactment of surveillance, a subjectivation of power, as instilled in prisoners who architecturally speaking must assume ubiquitous surveillance, that they may be under inspection at any time, night or day." This notion of enforced self-discipline has very much become a dictum for scholars studying surveillance – especially as contemporary surveillance practices through the digital realm have become indirect and remote. As Haggerty and Ericson (2000) argue, data are now easily collected, disassembled, circulated, and eventually re-assembled for a variety of purposes. In such fashion, individuals are digitally encoded, with analytical relevance ultimately assigned to their "data doubles." To stay within the metaphor: the panopticon has long lost its walls and has become an integral part of everyday life. Such a notion will be taken up by [Inquiries 1; 6].

The social implications of a digital and increasingly invisible everyday-panopticon are massive. As Monahan (2006a: 12) claims, "a 'panoptic' effect on social behavior, meaning that people tend to police themselves and refrain from any actions that might verify their presumed status as deviants in the eyes of unseen others." Individuals must then constantly question themselves in terms of the implications someone might derive from their data profiles. An analysis of surveillance must not be limited to the individual level, however. As indicated before, surveillance has become an effective political mechanism for the ordering of the social, most notably through the capacity to measure, sort, and classify populations. As Lyon (2006c: 221) emphasizes, "garnering personal details without the individuals concerned knowing about – let alone consenting to – it has become routine", and subsequently has the power increased that is generated by surveillance. The scale of surveillance has risen from particular groups to whole populations and has enabled wide-ranging schemes of social sorting (Lyon, 2003d). Surveillance as social sorting has become closely intertwined with security politics.

As Amoore and de Goede (2005: 150) argue, "what is new about contemporary terrorist risk management […] is its increasing reliance on technology and computerised data-mining." Surveillance, or rather dataveillance, potentially captures and stores information about whole populations, and enables security politics to exploit large-scale databases in order to create security-related insights that had not been accessible on such a level before – "security becomes digital and follows up traces left by everything which moves (products, information, capital, humanity)" (Bigo, 2008b: 109). The insights of surveillance-based analytics, however, must from an epistemological standpoint necessarily be regarded as mere potentials. [Inquiry 6] engages in-depth with such issues of knowledge generation through algorithmic analytics in PNR data. At this point, the narrative of security as surveillance strongly re-connects with the third narrative that analyzed security as future. Surveillance, in a sense, is the enabling mechanism for the creation of futures – be in preventive, precautionary, or preemptive modes of reasoning. Since in a worst-case scenario, any part of our everyday lives has been captured and encoded through digital traces, location-based services, communication and consumption profiles, futures can be extrapolated on both individual and collective levels – or at least so the argument put forward by security professionals goes.

The ordering of the social empowered by surveillance works through the classification of potential futures. In other words: security as surveillance works as *profiling*. Subsequently, "as sociotechnical systems, then, surveillance and security are intimately intertwined with institutions, ideologies, and a long history of social inequality" (Monahan, 2006a: 10). The profile itself rests on the applied mode of addressing the future – be it through archival-statistical forms of knowledge that are grounded in past experience, or through radically open forms of knowledge construction that rely on algorithmic analytics and the creation of possible connections between distinct types of data, as put forward by [Inquiry 6]. However, as Lyon (2006c: 224) argues, "many surveillance schemes that operate today tend to amplify stereotypes and to apply the most stringent and severe scrutiny to the most vulnerable – in socioeconomic, ethnic, and gendered terms." Surveillance can thus become a technique of singling out and disadvantaging certain parts of the population.

Scholars have however struggled with the panoptic notion of a central node where surveillance-powered analytics would converge, and where ultimate power would be created. With the ubiquity of contemporary surveillance, the figure of the panopticon has thus been profoundly challenged. Whereas in its original design, power was indeed centralized in the

prison control room, the societal analogy presupposes such centralized power in the form of the state. Surveillance, however, as has been pointed out, is not by any means limited to state authorities, but has become much more dispersed through a large variety of private companies and public-private partnerships. Scholars have thus increasingly drawn on another metaphor to describe the capillary systems of surveillance that characterize the digital age: the rhizome. Originating in biology and originally referring to the fragmented and de-centralized system of roots that certain plants (such as for instance asparagus, bamboo, or ginger) feature, Deleuze and Guattari (Deleuze, 1992; Deleuze and Guattari, 1987) have taken up the notion of the rhizome in order to highlight a number of features of modern societies. The figure indeed opens up the concept of surveillance to the limitless possibilities that have emerged through digital interconnectivity. As Deleuze and Guattari (1987: 7) have it, "any point of a rhizome can be connected to anything other, and must be."

There are no prioritized nodes and hubs in the network – the rhizome grows and interconnects according to no particular logic, but through functional necessities and mere possibilities. Surveillance, if we accept this notion, then must be conceptualized as a multitude of fragmented, dispersed, and flexible processes without an overarching agenda or a center of power. The narrative of security as surveillance re-connects here not only with the creation of futures, but also with the narrative of security as government that highlights the multiplicity of actors in both the political and the social. It also re-connects to questions of normativity when it comes to limiting and controlling surveillance in the first place. Scholars of surveillance have never been shy to make use of pop-cultural references and dystopic scenarios in order to highlight such a need. Movies such as Steven Spielberg's *Minority Report* (2002) and novels such as George Orwell's *1984* (1949) by now have a long history as anecdotes in academic work, as they depict a bleak outlook into a world that would be ultimately defined by, and governed through, surveillance. Arguably, the reason for this is the detrimental potential of surveillance and its recorded increase, which can easily be expanded to worst-case scenarios in which human rights and civil liberties will have become discarded for the sake of ultimate control – framed under the premise of security.

If surveillance must be thought of as an array of distinct, yet loosely connected and overlapping networks, then moral and legal accounts of its possible detrimental effects have become dispersed as well. Subsequently, [Inquiry 6] questions the applicability of the current legal framework when it comes to analytics-induced discrimination. Here, the narrative of security as surveillance re-connects to questions of the legitimized production of security and the role of the state that have been tackled in the last narrative as part of thinking about governing in terms of governmentality and governance. A further set of concerns emerges from the increased invisibility and everyday routinization of surveillance, as well as from the quickly emerging analytical possibilities of what is nowadays summarized under the label of 'Big Data'. As Jenkins (2012: 160) has it, "practices of social sorting are ubiquitous and far-reaching in modern societies, having gradually come to occupy a role at the heart of modern bureaucratic governance that is all the more potent because their taken-for-grantedness renders them almost invisible, part of the furniture of the state and business." Ultimately, surveillance practices possess the capacities to not only sort, steer and manage populations, but also to intrude into our spheres of intimacy and privacy in an automated fashion.

Sixth narrative: security as technology

As has been argued in the preceding narrative, surveillance is inseparably embedded in technological infrastructures and other technological means. However, such embeddedness of technology within society is not only the case for security as surveillance, but, more generally speaking, technologies play a prominent role in discourses and practices of security. Thus, this sixth narrative explores the implications of security as technology. Technology is a concept as vague as it is powerful, and, as Der Derian (1995: 25) claims, throughout history "in its name billions have been made and millions killed while scientific knowledge has been furthered and intellectual dissent muted." How come technology has been ascribed such a powerful role?

In terms of security, we must then ask: what is the role of technology in terms of how we come to understand and mold the world? How has it been shaped and negotiated, designed and rolled out? Which actors, interests and financial stakes have been involved in its creation processes? How is it implemented and used in everyday security contexts and how does that change the ways in which we interact with other humans and with our environment? Technology is in fact one of the main leitmotifs of the empirical section, and [Inquiries 2; 3; 4] particularly deal with some of those questions. The narrative of security as technology has been hitherto rather underexplored in comparison with some of the other narratives told in this thesis. As Guittet and Jeandesboz (2010: 229) point out, "while the uses and effects of technological systems are increasingly scrutinized by security scholars, little work has been done on the practice of technology itself with regard to security" – and surprisingly so. After all, technology has always played a central (however contested) role throughout the evolution of societies. There are a "wide range of claims regarding the status of technology in society" (McCarthy, 2013: 473), but most notably it has been connected with progress and wealth (and as such also with a notion of security conceived as the absence of scarcity). Thus, technologies have often had to enact the role of a redeemer that arrives to create a better world. As Monahan (2010: 92) argues, "at least since the Enlightenment, technologies have been wrapped up in a mythology of social progress, which frames any new advancement as an unqualified good." This very notion of the unqualified good, however, has in security studies more recently become increasingly challenged.

A supposed overall reluctance to overly criticize technology can arguably be retraced to multiple sources. As Edgerton (2007: ix) has it, "too often the agenda for discussing the past, present and future of technology is set by the promoters of new technologies" who possess the resources and power to actively shape public discourse and thus establish a positive notion of technology. Moreover, the widespread contemporary economic agenda of neoliberalism has also considerably catalyzed and reinforced a conceptualization of technology as an ultimate panacea for all of life's conceivable problems. As Harvey (2005: 68) puts forward, "the neoliberal theory of technological change relies upon the coercive powers of competition to drive the search for new products, new production methods, and new organizational forms" and as such appears closely entangled with the felt need to create monetary surplus. Underpinning such trajectories of constant search for new ways to impact markets and sell products, a more general desire for innovation can be identified – as Edgerton (2007: 209) critically argues, "to have technology or science is, it is often deeply felt, to create something new."

As Harvey (2005: 68) adds, "this drive becomes so deeply embedded in entrepreneurial common sense [..] that it becomes a fetish belief: that there is a technological fix for each and

every problem" – and most notably for security problems. This belief, as [Inquiry 3] retraces, is in fact deeply embedded in the European security agenda that strives to constantly produce new technologies in order to be able to compete at the level of a global security market. As has been laid out already, technology is indeed a cross-cutting phenomenon throughout most domains of security, be it the preemptive layer of counter-terrorism, the cooperative fight against transnational criminal networks, everyday policing tasks, or measures of preparedness and civil protection. In all of those domains we can find increasing reliance on technological support structures, queries in databases, sophisticated surveillance systems, and, maybe most importantly, constant calls from security practitioners themselves to roll out ever more technologies in order to render security operations more effective, efficient, and bullet-proof. Such technological fixes should however not be regarded as extrinsic or neutral. On the contrary, they must be carefully placed within the larger picture and analyzed in detail if we seek to understand the narrative of security as technology.

In fact, since the early 1980s, a whole new field of academic research has evolved around those very issues of technology and its role in societies. Science and technology studies (STS) have largely been concerned with the emergence and implications of the chain of research, innovation, design and resulting technologies, thereby focusing on social trajectories, genealogical knowledges and embeddedness in complex networks, and having produced a rich body of literature that security studies can benefit from. Among others, STS literature has focused on the role of agency in socio-technical assemblages that consist of human and non-human elements, raising questions such as: "When we act, who else is acting? How many agents are also present?" (Latour, 2005: 43), en route challenging the primacy of human security agents. Such scope on agency in non-human actors then necessarily presupposes a flat ontology that avoids *a priori* hierarchies and subsequently challenges the primacy of the human in the world on a more general level. Put simply: if we conceive non-human elements as "actants" (Latour, 2005) with the potential for creating a genuine impact on the world, then a whole new array of possible inquiries concerned with technology opens up. What is the role of algorithms, of automatic doors, of plain walls and fences, and so on? How do they shape and re-shape our perceptions of the world? How do the structure and re-structure the ways we act in the world? [Inquiry 2] empirically engages the social changes that were induced by the implementation of body scanners at a German airport security checkpoint, highlighting the surprising and unintended impacts that technologies can unfold. The narrative of security as assemblage will later once again return to such questions.

One must however be careful not to over-determine the role of technology and as such drift into a perspective from which technology becomes the dominant element of the social. As McCarthy (2013: 470) points out, such "technological determinism has loomed as the bogeyman […] for some 30 years", but scholars have begun to probe more deeply the role of technology as a means of power and government and its consequences for, for instance, concepts of identity and subjectivity. As Winner (2006: 278) argues, "there is growing awareness that technological devices, systems, and routines are thoroughly interwoven with the structures and processes of social and political life", thus necessarily placing inquiries into technologies on the agenda of critically thinking about security.

As Bigo (2012: 282) explains, in any study of security as technology, "the connection between person and machine, technological capacity and the will to use it to its fullest extent, whether resisted or otherwise, has to be appreciated in relation to historical and political figurations." Put differently: technology, in the realm of security, must also be conceived as a means of

governing and ordering the social that has historically evolved and transformed, however as one that easily escapes narrow political agendas and that unfolds more capillary (side) effects that must be carefully explored. One of the overarching phenomena of security as technology appears to be its potential as a connector/bridge between state agencies and private actors/the industry. As Murakami Wood et al. (2003: 144) point out, "governments and their military arms are now turning to software houses and technologists for more sophisticated tools to track and pre-empt crime and terror", and as such outsource not only issues of security architecture and design, but also willingly lose part of their political and agenda-setting power, while at the same time empowering (national) economies through the market.

Thus, security as technology appears to appeal to at least two (interlinked) grand notions: technology as general progress and technology as a means of creating wealth through industrial innovation. Some scholars, however, have uttered doubts about the first notion, as it can be read as derivative of the latter, and moreover as it seemingly becomes overshadowed by (intended as well as unintended) negative impacts of technology that would reverse or even pervert the broad notion of progress. As Haggerty (2004: 392) claims, "where modernity manifests a general trust in the ability of science to resolve our most pressing problems, we have become attuned to the truth that science itself poses risks and that these risks can no longer be explained away as temporary aberrations in the march of progress." As argued earlier, technology has proven to be a powerful domain of government. Or, as Rose (1999: 51) puts forward, "thought becomes governmental to the extent that it becomes technical, it attaches itself to a technology for its realization." Subsequently, critical thought must open up technology for close scrutiny in order to come to terms with its effects.

Thus, what are the (normative) implications of such governmental reason through technology for the purpose of security? First of all, as Harvey (2005: 69) points out, the neoliberal logics of market dominance have become a threatening force, since "technological developments can run amok as sectors dedicated solely to technological innovation create new products and new ways of doing things that as yet have no market." For instance, such an angle has been increasingly attributed to the security research framework of the European Union and its quasi-exclusive scope on the development of new technologies in order to create wealth surplus for the European security industry and subsequently for the overall economy. As de Goede (2011: 10) points out, "the European Security Model is fostered through research funding and market integration. A flavour of such cultural invocation of disaster scenarios, coupled with the promise of a technological security fix is given in the FP7 brochure on current EU security research", leading to a deliberately simplistic conceptualization of security that could be realized if we just put more money into research and innovation – a notion that is critically dealt with in [Inquiries 1; 3]. As was programmatically argued by multiple fora constituting EU security research: "technology will play an important part in each nation's counter-terrorist efforts" (European Security: High Level Study on Threats Responses and Relevant Technologies, 2006: 3), starting from the assumption that "technology itself cannot guarantee security, but security without the support of technology is impossible. It provides us with information about threats, helps us to build effective protection against them and, if necessary, enables us to neutralize them" (Group of Personalities in the Field of Security Research, 2004: 7). The next narrative will engage this thematic at greater length.

A second strand of critique towards security as technology has evolved around the potential of establishing threatening and insecure affective states. As Burgess (2009: 316) explains, "the management of insecurities through technology and the development of new technologies of

security are increasingly becoming policy priorities for the EU and its member states." Technologies have been conceived of as primary means for enacting a preemptive state of mind through the wide-spread roll-out of distinct registers of risk. As O'Malley (2004: 1) frames the issue, "risk frameworks form the basis of regimes of security that attempt to turn each of us into crime prevention practitioners and in some case to turn our homes and even communities into hi-tech fortresses." Risk, in such a fashion, re-distributes accountability for canceling out the ominous 'event' to every single member of societies, while at the same time offering a subtle solution to overcome such burden: purchase and rely on technology. Conceived through such a lens, the narrative of security as technology strongly re-connects to previous narratives of security as future and security as securitization. Technology, so the argument goes, enables us to both to obtain (more precisely: feign) control over contingency and thereby assists to colonize ever more areas of politics. In this vein, security as technology again draws on the notion of security as surveillance. As Burgess (2009: 316) argues, "new technologies of control and surveillance, which rely in particular on evolutions in technologies of information and communication (TICs), are deemed crucial in this perspective because they allow agencies to anticipate threats and act proactively instead of being limited to reactive measures."

We should, however, keep in mind the claims made in the literature on governance and governmentality, as well as insights from the field of STS. As has been pointed out in the previous narrative of security as government, a notion of governing according to a master agenda, be it through technology or through any other means or technique, is an overly simplistic one. As Rose (1999: 53) reminds us, "technologies are not realizations of any single will to govern", but they come into being through multiple and intertwined trajectories and actor constellations. Thus, the question for any (critical) research on security as technology then must be to explore which stakes are reflected and which are marginalized within any specific technological flight of path – after all, "it is not that technology develops outside of human agency, but that it develops outside of *some* humans' agencies. The ability to control technological design and development is a significant facet of social power relations [emph. in orig.]" (McCarthy, 2013: 476). Thus, at least for STS, a main line of the agenda has always been about the "need to emphasise the social, political and historical context when detailing the design, development and diffusion of technological artefacts" (McCarthy, 2013: 478). In order to do so, Latour (2005: 80) suggests to "study *innovations* in the artisan's workshop, the engineer's design department, the scientist's laboratory, the marketer's trial panels, the user's home, and the many socio-technical controversies [emph. in orig.]" that (security) technology is exposed to throughout its emergence. [Inquiry 1] attempts to provide such an account through the study of the interrupted roll-out of body scanners in Germany, tracing such interruption to a necessary re-design due to public concerns in terms of privacy and intimacy.

After all, it is the "little security nothings" (Huysmans, 2011) mentioned earlier, that are so deeply embedded in our everyday lives, and that have been subjected to the multiple centrifugal tears of distinct actors interests and claims. As Lyon (2006c: 210) frames the issue, "taken-for-granted technologies have far-reaching implications for power relations within the modern, bureaucratic, capitalistic contexts where they were developed" and must therefore be researched carefully. However, to unveil such power relations can prove to be difficult – especially when it comes to the domain of highly sophisticated technological infrastructures that tend to present themselves as black boxes of proprietary and seldom traceable algorithms that nonetheless "instantiate the values, epistemologies, and ontologies of their creators and impose them on their subjects" (Bennett et al., 2003: 155). Once again drawing

on the notion of a messy assemblage rather than a clear-cut divide across domains such as the public/the private or the state/the economy, we must then not only think about the emergence of technologies, but also about their agenda-setting capacities on the political and the social level.

As Huysmans (2006: 8) points out, "the solutions and available technologies do to some extent define the problems and they develop to some degree independently from the politicization of events." In this vein, technologies seem to supersede and potentially cross any straight-forward political agenda. Not openly, however, but through a subtle creep that constitutes the core of the research program of the Paris school of securitization. In such fashion then, "much like legislation, technological systems provide a set of rules, or scripts, encouraging certain uses or interactions and discouraging others" (Monahan, 2010: 93), thereby unfolding discriminatory and marginalizing notions that need not be directly linked to a political program, but rather emerge through the dispersed, yet entangled, field of security professionals and the industry. Thus, in an attempt to link the hitherto rather seldom connected research programs of STS and security studies, Huysmans (2006: 13) suggests to "push security studies in the direction of a sociology of the technocratic politics of insecurity in which discursive processes are embedded in technological and professional processes and struggles." This appears indeed a necessary move. After all, "software-driven systems are allowing further industrialization of everyday life through what appears to be a combination of the physical and virtual, leading to both spatial (territorial) and analytical (information-based) exclusion" (Murakami Wood et al., 2003: 142), as has been indicated by the preceding narrative of security as surveillance.

Seventh narrative: security as economy

The sixth narrative has explored how the notion of security is shaped and re-shaped through the lens of technology and how technology is framed as an innovative driver for better security (and subsequently for a better society). Moreover, it has shown that a positive framing of security technologies has been rightfully contested by pointing out the detrimental potential of many technologies, especially large-scale data-based systems of monitoring and calculating. Along the way, we have already touched upon a crucial issue within such a conceptualization of security as technology: its *economics*. This seventh narrative zooms in more closely into this field and tells the story of security as economy. In fact, "we find numerous technologies introduced on a rapidly evolving basis, from ever more sophisticated surveillance cameras, to biometric identification and verification systems, full body scanners to motion detection systems" (Kroener and Neyland, 2012: 141), and tracing the underlying monetary rationales of this phenomenon arguably allows us to understand another layer of security. As Hayes (2012: 167) quite plainly frames the issues at stake here: "in the post-9/11 security focused world, surveillance is big business." Such business builds on the transformation processes that have rendered "the contemporary field of security [..] transversal not only to the inside/outside distinction, but also to the public/private distinction" (c.a.s.e. collective, 2006: 464), thereby opening the door for a security business case in the first place.

And yet the business aspects of security, although more recently critically discussed by scholars such as Hayes (2006; 2009; 2010), Klein (2007), de Goede (2011), Bigo and Jeandesboz (2010), or Zedner (2006a), remain rather underappreciated within the field of security studies. As Klein (2007: 306) points out, "what is most striking is how little the security boom is

analysed and discussed as an economy, as an unprecedented convergence of unchecked police powers and unchecked capitalism, a merger of the shopping mall and the secret prison." Thus, how can we make sense of such neglect to study security as a means of profit generation? One reason for this might be that, in fact, an entanglement between security politics, technological means, and strong industrial lobbyism is not by any means something new and thus not a field that would yield many new insights. However, as often as not, 9/11 can be conceptualized as a crucial event here, that catalyzed long-term tendencies and provided a window of opportunity for the industry to make unprecedented business pitches. As Lyon (2003c: 18) argues, "high-tech companies, waiting in the wings for the opportunity to launch their products, saw September 11 providing just the platform they needed." It imminently appeared rather clear that security politics would undergo significant adjustments, and the private sector counted on the fact that the "global market for technologies of repression [would become] more lucrative than ever in the wake of 11 September 2011" (Hayes, 2006: 3). Moreover, public discourse was heavily influenced by the industry. As Lyon (2003c: 18) notes, "not surprisingly, almost all the 'experts' on whom the media called for comment were representatives of companies."

There was always money to be made through uncertainty. Be it through simple door locks, through alarm systems and surveillance cameras for private homes, or through wholesale, large-scale databases and analytics that are developed directly for (and procured by) state agencies. Especially the latter has been a matter of concern for many critical scholars. As Hayes (2012: 167) summarizes the problem, "governments outsource key aspects of security and surveillance policy and practice to the private sector, subsidize private innovation in surveillance capacities and techniques, and procure the resulting technologies and expertise – all of which is to the dubious benefit of both untrammeled state power and hose private corporations and actors best placed to profit from this relationship." Thus, governmental agency is deliberately re-located, resulting in complex, and most notably proprietary, security solutions such as software packages for data-mining or 'smart-CCTV' systems that define deviance in opaque and non-retraceable ways.

What we find here is indeed a close link to the narrative of security as securitization. For the sake of selling a security *solution*, there must first be a security *problem*. Thus, as de Lint and Virta (2004: 472) point out, "security economies come to depend on the regular identification of new risk markets that may sustain the appetite for security production." Threats, in this vein, come to be constructed partly through a private sector that has no real interest in actually *solving* such security 'problems', but rather in *maintaining* them such that there can never be a market saturation that would delimit sales. As Schouten (2014a: 28) argues, "those who claim to be in the business of providing security represent it by *other* things, which are then 'packaged' and 'sold' as containing threats of promoting security [emph. in orig.]." Subsequently, global corporations have vital stakes in new threats, in larger risks, and eventually in radical contingency interpreted as constant danger. In this vein, "private security specialists prepare the world's 'hot spots' for TNC [transnational corporations] profit making" (de Lint and Virta, 2004: 471), and governments appear to be willing to align with such a mapping of the world. As Hayes (2009: 80) rather sarcastically puts it: "the new public-private partnership for homeland security is based on a simple *quid pro quo*: profit for companies and power for states [emph. in orig.]."

Security as economy must however be careful not to fall into the trap of reductionism. As Walters (2012: 24) reminds us, an exaggerated notion of the economy runs the risk of painting

a "theoretically and ontologically impoverished image of a world characterized in its entirety by neoliberal capitalism. There is much more to the world than neoliberalism." This is certainly true, and throughout the preceding narratives we have seen that there is much more to the complex notion of security than simply profit-making. Nonetheless, and keeping this warning in mind, the rather limitless contemporary mode of neoliberal economics has drawn considerable critique for its all-encompassing tendencies – security included. As Harvey (2005: 3) claims, "neoliberalism has, in short, become hegemonic as a mode of discourse." When considering a world that is stacked with countless security measures that deeply extend into our everyday lives, then such a neoliberal lens on security appears not that far off. Indeed, how else but in a neoliberal fashion can we, as Hayes (2009: 78) drastically puts it, "conceive of a world characterised by mandatory surveillance and wholesale risk profiling"?

Neoliberal economic theory in fact strikingly resembles a conceptualization of security as futurity through risk. Both, in the vein of Beck, presuppose a model of a laboratory-like, theoretical equilibrium which might even perfectly work if not for the messy nature of the actual real world. As Harvey (2005: 68) puts it, "the neoliberal presumption of perfect information and a level playing field for competition appears as either innocently utopian or a deliberate obfuscation of processes that will lead to the concentration of wealth and, therefore, the restoration of class power." Neither is the notion of risk anything but utopian for any meaningful prediction of the future, and we might actually say that it restores power not necessarily in terms of class, but in terms of government. Or rather in terms of governmentality, that is. As has been shown earlier, governing must be conceived of as a dispersed array of techniques and actors – and in terms of political agency the security industry must in fact be thought of as one such actor. Albeit a powerful one.

The entanglement of the private sector and the political level has been shown quite compellingly when it comes to the emergence of security within the European Union, and more particularly the EU's Security Research Programme that, as Hayes (2009: 4) puts it, "continues to be shaped by prominent transnational defence and security corporations and other vested interests." In the wake of 9/11, the EU sought to establish its own research program specifically dedicated to security solutions, and for the sake of exploring its feasibility, in 2004 a "Group of Personalities in the Field of Security Research" (GoP) was assembled, which however was comprised mostly of representatives of large European security and defense companies (Bigo and Jeandesboz, 2010). Their report came to the conclusion that "Europe needs to act quickly if it is to remain at the forefront of technology research, and if industry is to be able to exploit the results competitively in response to the rapidly emerging needs for sophisticated security-related products" (Group of Personalities in the Field of Security Research, 2004: 13), thus calling for swift political action – however not necessarily for the purpose of better security, but for the purpose of making a better business case out of the current desire for all kinds of security measures.

Two years after such foundations had been laid, the GoP was succeeded by the newly formed "European Security Research Advisory Board" (ESRAB), which once more highlighted the fact that security technologies "could offer Europe a competitive advantage in a global market" (European Security Research Advisory Board, 2006: 28). Three more years later, the ESRAB was eventually followed up the "European Security Research & Innovation Forum" (ESRIF) which reinforced the presupposed need of "promotion of innovation as the foundation for a European security market that exploits economies of scale at European level" (European Security Research & Innovation Forum, 2009: 11). Thus, the emergence of the EU's Security

Research Programme was closely entangled with the private sector – at the same time developing the general agenda and promoting their own stakes in the development of new technologies that would make profitable sales in a global market constituted by insecurity and terrorist threat. As Hayes (2009: 78) summarizes the intervention, "a small group of military-industrial companies came together to secure substantial R&D subsidies for EU homeland security."

In fact, what becomes rather clear throughout the documents that had been produced by the distinct fora along the process, is the clear-cut economic agenda that appears less interested in the fact *what* is to be sold than in the fact *how* it can best be sold. As pointed out by ESRAB, "economic theory in particular can offer key insights, enabling governments to optimize their efforts to enhance security and growth" (European Security Research Advisory Board, 2006: 59), and moreover, that "in order to stimulate the demand for new and innovative security products and services, incentives for public authorities, often seen as 'first buyers', should be introduced" (European Security Research Advisory Board, 2006: 71). Such rationales appear very much inspired by the neoliberal primacy that markets produce virtues (profits), and "if markets do not exist […] then they must be created, by state action if necessary" (Harvey, 2005). Thus, in order to establish a security market, ESRIF in fact proposed that "analogous to environmental regulation which enables firms to profitably contribute to 'green growth', one can think of regulation that stimulates 'secure growth' by enabling industries for security-enhancing products or services" (European Security Research Advisory Board, 2006: 59).

Such dominance of the private sector, especially in an area as sensitive as security research, and subsequently security politics more generally, has garnered considerable critique. As Hayes (2012: 167) plainly frames the issue, "this is an undesirable relationship within which political decisions are shaped not just by democratic concern for the 'public good' but by profitable courses of action for private entities", and as such undermines the normative obligations of government. In fact, security conceived through the lens of the imperative of the economy appears very much reduced to the Paris school argument about governing through *insecurity*. In order to extract as much monetary surplus from security as possible, its inherent pathological tendencies must not only be slowed down, but also considerably extended. In other words: security as economy benefits largely from securitization.

Private sector impact arguably touches even upon the legal system. As Zedner (2006a: 268) argues, "in the field of security, technological and global capital developments also create more elusive and inconstant sources of control than the edifices of the criminal law and the criminal court." To be quite concise here: there is no fault *per se* with private sector engagement in political processes – this has in fact always been a part of politics. Rather, the problem here lies in the *excess* of interventions from the industry into the policy field of security, which must be handled with care. As Harvey (2005: 79) explains the issue, "at the heart of the problem lies a burgeoning disparity between the declared public aims of neoliberalism – the well-being of all – and its actual consequences." In this case, such consequences entail the implementation of multiple technologies of surveillance and control into our everyday lives. The potential detrimental impacts of such tendencies have been outlined in the preceding narratives of security as securitization, as surveillance, and as technology.

Eighth narrative: security as assemblage

As has become apparent up to this point, security comprises of a multiplicity of meanings, some of which have been retraced through overlapping stories that are used to 'tell' security politically. Security is continuously transformed, calculated, and encoded. Security is continuously enacted, imagined, and technologized. Security is continuously performed, routinized, and bureaucratized. And security is continuously reasoned, dispersed, and privatized. This last introductory narrative aims to reflect upon those multiple meanings and overlaps that turn security into the messy empirical and intellectual field that we encounter today. As Geyer (2008: 2) summarizes the issue, "even for professional observers, it is difficult to even glimpse the 'security web' that is currently being spun at national, supranational and transatlantic levels alike." This eighth narrative is about security as *assemblage*. It draws mainly on literature from the field of STS, but also incorporates more recent developments that have been termed as "new materialism, immanent naturalism, posthumanism, antihumanism, speculative realism, complexity theory, object-oriented metaphysics, a philosophy of becoming" (Connolly, 2013: 399), and arguably in even more, shiny ways that highlight the "multiple connections across myriad technologies and practices" (Haggerty and Ericson, 2000: 609).

Foucault (1980: 194) has famously outlined what such an assemblage can be about. What he has deemed a "dispositif" embodies a "heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions." Be it framed as assemblage, as dispositif, as apparatus of security (the most common English translation of the French term dispositif), or as rhizomatic network (Deleuze and Guattari, 1987) – decisive for such an understanding of security is the acknowledgement of the complicated state of things, requiring an ontological stance that comes to terms with "multiple overlapping sites of production of sovereign power (public, para-public and private actors) constitute *in actu* the security apparatus [emph. in orig.]" (Guillaume, 2014: 109). In fact, the notion of security as assemblage closely links to the notion of security as government(ality) in its relational conceptualization of power. However, it advances beyond the rationalization strategies of government. As Lisle (2014: 70) argues, "assemblage thinking does not accept the subject/object distinction that orders so much of contemporary life and allows us – as researchers – to isolate the targets of our research and subordinate them through our methods of inquiry."

In the words of Latour (2005: 25), "controversies are not simply a nuisance to be kept at bay, but what allows the social to be established and the various social sciences to contribute in its building." Controversies as such must then become the focal point for academic analysis. Not looking to settle ambiguity and contradiction, but on the contrary seeking to extract added value from them, "assemblage thinking offers an approach that is capable of accommodating the various hybrids of material, biological, social and technological components that populate our world" (Acuto and Curtis, 2014: 2). Put very simply: assemblage thought, which Acuto and Curtis (2014: 3) deem "less of a *theory* and more of a repository of methods and ontological stances towards the social [emph. in orig.]", starts from the assumption that there is no primacy of human agency in the world, but only "complex relations between the human estate and a host of nonhuman processes with variable degrees of agency" (Connolly, 2013: 400). The question of agency has most notably been one that STS has been concerned with – and one that becomes important for security studies with regard to the manifold security

controversies and negotiations that we encounter. How can we conceive, for instance, of the role of the algorithm or the automated biometric gate and their status in human/non-human setups? How can technology lead or prescribe human action? And through which processes did the algorithm or the gate evolve in the first place? Such questions have been rendered highly important for thinking about security. However, as Schouten (2014a: 26) states, assemblage thought "is only sparsely explored in security studies." How can it provide help, then?

In order to explore questions of agency in socio-technical assemblages, any assemblage-inspired analysis must carefully scrutinize the complex and unstable power relations between *all* elements of an assemblage, not merely between human actors. As Collier (2009: 80) explains, "a topological analysis focuses on the broad configurational principles through which new formations of government are assembled, without implying that they arise from some inner necessity or coherence." Such a topological analysis defines the boundaries of the field of research in the first place. But it must not stop at defining the field, but most importantly continue to analyze what is going on *inside* that field. As Latour (2005: 39) argues, security as assemblage needs to consider "the many contradictory ways in which social aggregates are constantly evoked, erased, distributed, and reallocated." Such an approach must necessarily start in the field itself – "assemblage thinking implies an empiricist project" (Büger, 2014: 59).

Especially actor-network-theory (ANT; for an overview see Latour, 2005) has both been criticized and praised for its presumed flat ontology that proceeds beyond any *a priori* assumptions about how the world is structured and how action and agency constitute themselves – not necessarily through human conscience, but through the mediating forces of such mundane objects as, for instance, doors and walls, tools, or communication devices. The social, through this lens, appears as something that is emergent and contingent, and that is constantly re-defined by transforming assemblages. As Latour (2005: 5) points out with regard to such a conception of 'the social', "it's perfectly acceptable to designate by the same word a trail of associations between heterogeneous elements" rather than to reproduce the paradigm of 'classical' sociology that he blames of pre-structuring the social before researching it. In his account, all kinds of "mediators transform, translate, distort, and modify the meaning or the elements they are supposed to carry" (Latour, 2005: 39). As Acuto and Curtis (2014: 7) simplify the matter somewhat, "this ontology can provide a valuable starting point for the analysis of various social actors, including transnational corporations, institutional networks, epistemic communities, nation-states, cities and terrorist networks, which are often kept separate in theories founded on ontologies that make them incommensurable." In short: security as assemblage radicalizes the widening and deepening debates in security studies that have been explored in the narrative of security as (academic) transformation.

Through such a radical account, security as assemblage opens up a research agenda that builds on "relational ontology and post-Cartesian symmetry between people and things, discourse and materiality, the social and technology, and, finally, controversies in human and natural sciences" (Schouten, 2014a: 26). Such a notion builds a strong link to securitization theory as well. If, as Bigo (2008a: 32) has it, "the ban-opticon is [..] characterized by the exceptionalism of power (rules of emergency and their tendency to become permanent), by the way it excludes certain groups in the name of their future potential behaviour (profiling) and by the way it normalized the non-excluded through its production of normative imperatives, the most important of which is free movement", then we must disentangle how such an

assemblage of the ban emerges, transforms, stabilizes and, eventually, might disassemble again. In doing so, an analytics of assemblage must always keep in mind that, just like with the relational power approach in governmentality, "the elements of an assemblage may have a concerted or emergent effect without there being an underlying organizing principle" (Salter, 2013: 12). Such insight renders actual research both more easy and more complicated. On the one hand, research is made easier by simply venturing into the field without any predisposed restrictions or delimitations. On the other hand, however, if everything potentially can make a difference, then we constantly run the risk of missing out on some important element of an assemblage that unfolds power through unprecedented ways.

Thus, how are we to come to terms with an agenda of security as assemblage empirically, if its empirics are defined by radical openness? Connolly (2013: 401) suggests a clear-cut "problem orientation, pursuing the contours of an issue up and down these interacting scales, as the issue requires." If security politics evolve around specific security problems, in whichever of the manifold ways that we have sketched out so far, then the very evolution of complex, and at times contradictory, assemblages alongside the constitution of security politics provides a valuable starting point. As Adey and Anderson (2012: 106) argue, "in seeking to understand how life is governed in and through contingency, we should take care to remember the contingencies of the apparatus of security – that is, how apparatuses form, endure and change as the elements that compose them are (re)deployed." Already implied in such a perspective is the notion that each assemblage could be formed differently – and that what we encounter is merely a momentary snap-shot of stabilization that might rather sooner than later fall apart again through the multiple contestations that security is subjected to. As Schouten (2014b: 88) claims, such a perspective could considerably contribute to a general agenda of thinking about security by "by radicalizing the insight in security studies that security is 'essentially contested' to study the on-going attempts to stabilize security." As he adds: "if security practitioners 'out there' struggle with the very ontology of (in)security, how could 'we' as analysts a priori decide that security is a matter of discourse, practice or materiality?" (Schouten, 2014b: 88)

The utility of such an approach becomes rather obvious when we call to mind the preceding narrative of security as economy and the ensuing "close assemblage with international partners and private companies that underpin the EU's force in the domain of security" (de Goede, 2011: 12). Moreover, it can also contribute to the multiple layers of security as surveillance and technology, as government, and as futurity and securitization. Security as assemblage, however, is not some kind of 'master narrative'. Neither does it occupy a privileged position among the narratives of security provided here. Rather, thinking about security as assemblage can arguably contribute to a better understanding of how all of those narratives come into being empirically – not necessarily through an underlying political agenda, but through complexity, fragility, and ambiguity. With regard to security, then, as Schouten (2014a: 28) explains, "this process of translation concerns ontological *politics*, for establishing security as technical rather than social, or private rather than public, subsequently restricts and redefines accountability; distribution of scarce output; and/or the scope of possible action available to different affected actors [emph. in orig.]."

After all, as Rose (1999: 22) reminds us, "the space of government is always shaped and intersected by other discourses, notably the veridical discourses of science and changing moral rhetorics and ethical vocabularies, which have their own histories, apparatuses and problem spaces, and whose relation to problematics of government is not expression or

causation but translation." It is this very translation that must be researched empirically if any analysis seeks to unpack specific security assemblages. The processes of translation mark the trajectories along which actor relations form and re-form, and, most importantly, become visible: "when security is in the making – that is, still a controversy to be settled – it is ontologically unstable and indistinguishable from the 'context' made up of economic, technological, medical and legal considerations" (Schouten, 2014a: 38). Scholars of governmentality have shown that "an analytics of a particular regime of practices, at a minimum, seeks to identify the emergence of that regime, examine the multiple sources of the elements that constitute it, and follow the diverse processes and relations by which these elements are assembled into relatively stable forms of organization and institutional practice" (Dean, 2006: 21), and thus we can once more identify a strong parallel here.

As Rose (1999: 277) quite plainly frames the issue, "our present has arisen as much from the logics of contestation as from any imperatives of control", and thus security studies must in fact transcend the scope on control that strikes at the heart of many inquiries into surveillance and technology. In the vein of Foucauldian thought, as Schouten (2014a: 38) emphasizes, the "critical purchase thus lies in offering us a way to study security, not in terms of stable arrangements that impress themselves upon us as powerful 'cold monsters', but rather as unsettled accounts of fragile security by entering in to the controversies when security is still in the making." What implications must be derived from such insight? How does this narrative of security as assemblage undermine, underpin, challenge, or reinforce its preceding narratives? It most certainly thwarts any over-simplistic understanding of security that centers merely centers around selected rationalities, thereby neglecting others. It can serve to highlight how economics or technological discourses have prevailed in the arena by tracing how, and through which particular power relations, controversies and ambiguities have become settled and stabilized. And by doing so, it can most notably challenge security *politics* by exposing reductionist and epistemologically twisted arguments of governing, of securitization, and of futurity. As Connolly (2013: 404) rather ironically puts the added value of assemblage thought: "'How come we did not anticipate this?', ask the Intelligence agencies. 'How come we did not predict this?', whisper political scientists to each other, before they catch themselves to recall how they only promise to predict hypothetical events under conditions in which the 'variables' are closely specified, and not to explain actual events in the messy, ongoing actualities of triggering forces, contagious actions, complex and floating conflicts, creative responses, obscure searches, ambiguous anxieties, and shifting hopes."

One crucial question remains. The question that concludes this first section: what insights for security as such, if any, can we gather up to this point? I would like to propose two rather banal findings. *First*: the narratives of security told so far have not exactly served to clarify matters. On the contrary, they have complicated things, culminating in a conceptualization of security as assemblage that in a way radicalizes the openness and fluidity of security that was highlighted from the very outset of this thesis. This is deliberately so. Once more, we should keep in mind that each of the narratives is more or less capable of standing on its own. And moreover, that many of the narratives have indeed been researched exactly as this – as a stand-alone perspective that strives to rationalize security alongside disciplinary delimitations or selected angles. However, one major goal within section I. has been to overcome such fragmentation in order to provide a more nuanced, more detailed, but most importantly, more holistic framework of security. It could even be argued that one might find an almost

linear trajectory throughout the consecutive narratives, starting from the simple anthropological search for security and ending up with the highly complex, complicated notion of assemblage. What such complication implies is the pressing need for empirical research. *Second*: the narratives of security told so far are for the largest part devoid of such empirical underpinnings and remain on a rather abstract, theoretical level. Just as well, this is deliberately so. The empirical underpinnings necessary for any meaningful take on security will be provided by the analytical pieces that are to follow in section III. They will explore matters of databases and algorithms, matters of privacy and data protection, matters of risk and imagination, matters of business and the industry, matters of professionals and authority, matters of research and technologies, matters of outsourcing and the private sector, matters of surveillance and profiling, and matters of governing and reasoning – in short: they will explore many of the registers of security that we can find throughout aviation. Before going on to do just that, however, the next section (II.), will briefly plunge into questions concerning this very field aviation. Put very simply: *why research the airport?*

II. Interlude

“I remember when flying was enjoyable.”
(User “KTD”, 22 September 2011, www.flyertalk.com)

Stories from the airport

On 17 April 2012, a man, later identified as John E. Brennan, created major headlines as he went through security screening at Portland International Airport. As reported by "The Oregonian", a Portland-based newspaper, Brennan stripped completely naked in order to protest against intense and invasive screening procedures. After taking off all his clothes, Brennan proceeded to walk through the checkpoint entirely naked and was eventually taken into custody by local police authorities and later accused of public nudity and disorderly conduct.

Why study the airport? As has been indicated at the very beginning, security creates friction – and arguably there are few places where this friction can be experienced as intensely as at the airport. Airports have clearly been one of the focal points of security reinforcements in the last decade. As Schouten (2014a: 23) points out, "since 9/11, terrorism has turned their security into a global controversy. Airport security has become a central preoccupation of security practitioners worldwide." The little sketches of actual real-life 'stories from the airport' illustrating this section are rather randomly picked incidents (similar to the many others which can be found throughout the news archives if one is willing to dig), but they suffice to highlight the conflict potential of tightened screening protocols, attempts to profile travelers in advance of their actual journey, and new, invasive technologies such as body scanners.

Thus, why is security politics so locked in at the airport? *First* of all, airports have been the point of entry for the attacks of 9/11, and this very fact is regularly being recurred to by discourses of security. As such, airports have been rendered iconic for security. *Second*, airports are highly particular spaces of transit that lack many aspects of social cohesion that we can find in the 'regular' spaces that we inhabit on a regular, everyday basis. As Lyon (2003a: 13) dubs them, "airports are 'placeless' sites of temporary sojourn, air-lock chambers for nomadic executives or sun-seekers." Such "non-places" (Augé, 2006) of transit, only temporarily passed through by strangers, are arguably more likely to foster an atmosphere of mistrust and suspicion that must be, so the argument goes, countered by stricter security measures.

Which leads us to the *third* characteristic: airports feature 'more' security than most other spaces. More security in terms of surveillance and control technologies, more security in terms of capturing and storing data on individuals, and arguably stricter regimes of behavioral protocol. As Winner (2006: 281) argues, airports embody the "recognition that sociotechnical arrangements based on trust are also sources of insecurity [that] bought a widespread, highly costly refurbishing of many technological devices and systems." In short: airports are highly regulated environments. This does not imply an overarching security agenda for global aviation, or even for one single airport. On the contrary, and in the vein of security as assemblage, Schouten (2014a: 25) highlights that "myriad spokespersons enter stage and open the black box or airport security, turning it into a controversy composed of many unpredictable elements." However, notwithstanding such controversy which usually remains invisible to the occasional passenger, airports are epitomes of contemporary security regimes stacked with surveillance systems, technologies, police forces and private security guards, and as such have garnered a lot of attention from security studies.

Fourth, airports have been heavily marketized. Apart from being actual shopping-center like spaces of commerce themselves, airports are plain and simple an integral part of a global economy by providing the underlying infrastructure for worldwide trades and services, and as

such must be carefully protected as part of the critical infrastructure that enables our way of life – or so the common argument goes. Moreover, the provision of security at airports has also been subjected to transformations. As Schouten (2014a: 29) points out, "security governance at airports and elsewhere is performed not primarily by state security forces, but rather by networks of security actors that cross-cut public/private, local/global and formal/informal dichotomies", thus introducing a further commercial rationale into the complex assemblage of the airport. *Finally*, and connected to the empowerment of the global economy, aviation, like no other means of transport, is crucial to our modern lifestyle that at times appears to be dominated by unlimited mobility. Such a scope on mobility has more recently been picked up by numerous scholars who emphasize that "mobility is no longer outside authority and government. Mobility itself has become part of new forms of authority and government" (Bærenholdt, 2013: 27) and as such strikes at the core agenda of studying security.

The Austrian firm Kontraproduktion shirts (www.kontraproduktion.at) is one of those online shops that sell supposedly funny t-shirts that engage with life's contradictions through mostly pop-cultural references. One of their products sticks out, however. In front of an airplane taking off, it shows a figure throwing a bottle into a trash can, with a slogan beneath it proclaiming: "Throwing away my half-full bottle of water won't make your world more secure" ("Das Wegwerfen meiner halbvollen Wasserflasche macht eure Welt nicht sicherer"). More sarcastic than humorous in its message, the shirt in fact pinpoints one of the major debates around airport security in recent years. The ban of liquids – with the exception of separately packaged containers that do not exceed 100ml – has been deemed as one of the most striking examples of highly symbolic security politics without any real world impact. Indeed, to some, it appears so absurd that it has now even found its way on to t-shirts.

The 'stories from the airport' that entitle this section have to be understood in a two-folded fashion. The brief anecdotes provided here are such stories that illuminate the friction that security at the airport creates every day around the globe. Just as well, however, the analytical pieces that constitute the next section (III.) are in some sense such 'stories from the airport'. They are empirical takes on how airport security comes into being, how it plays out, how it is contested and stabilized, how it is made and re-made. In fact, airport security emerges and re-emerges around the narratives of security that we have explored in section I., and a considerable amount of recent research has attempted to explore such issues. Be it the fact that airports must be conceived of as complex assemblages of security that undergo constant controversies, re-evaluations, negotiations and subsequently transformations (Lippert and O'Connor, 2003; Salter, 2008c; Schouten, 2014a). Be it the fact that airports have become a focal point of governing mobile populations through a multitude of modes of power and authority (Salter, 2007). Be it the fact that airport security desperately strives to render the future actionable in order to prevent the next event of terrorism through hi-jacking or bombing and thus has become the center of attention for scholars engaging anticipatory politics (Salter, 2008b; Adey, 2009). Be it the fact of complete surveillance of airport spaces in both physical and digital terms and the discipline and social sorting it enacts in the name of security (Bennett, 2005; Adey, 2004b; 2006; Adey et al., 2012; Klauser et al., 2008; Lyon, 2008). Be it the dominant role of security technologies for purposes of identification, access management, and scrutiny at the airport (Lloyd, 2003; Cavoukian, 2009b; Jones, 2009; Tugas, 2013). Be it the multiple securitization processes that aviation has been subjected to (Salter, 2008f). Or be it the fact that airport security in many parts of the world has been liberalized,

privatized, and out-contracted (Hainmüller and Lemnitzer, 2003; Seidenstat, 2004; O'Malley, 2006).

In summary, airports can be conceived of as emblematic for a liberal mode of governing that is preoccupied with the empowerment of global flows. Flows of people, goods, services, money, and data, that is. Those flows, however, must nonetheless be closely monitored and regulated for the sake of security. As Lyon (2006c: 218) argues, "post-9/11 antiterrorist tactics include these three areas: travel, focusing on security at airports and borders; financial systems, focusing on curtailing the flow of funds to 'terrorists'; and communications, focusing on the interception of suspicious messages", all of which are domains which thrive on the paradigm of circulation. Mobility, however, has arguably garnered most attention, since its modulations in terms of monitoring and profiling, and in terms of analyzing and scrutinizing can be directly felt by any traveler – having turned global connectivity into some kind of gauntlet run. After all, in order to be granted the smooth and uninterrupted journey that is promoted in aviation's advertisements, one better not stand out from the crowd in some suspicious fashion – be it behavior, be it dangerous objects, or be it banal data characteristics such as past travel destinations, a cash-paid ticket, or the dietary choices for on-flight meals. As Bærenholdt (2013: 20) argues, "mobility is often associated with flow and freedom; nonetheless, it is also about power and government." Such an arguably odd marriage between lightness and regulation, between freedom and power, between circulation and stops becomes in fact much clearer when we underpin empirical findings from airport assemblages with Foucault's work on *biopolitics*.

Only one week after Umar Farouk Abdulmutallab, now widely known as the 'underpants bomber', had unsuccessfully attempted to blow up Northwest Airlines flight 253 from Amsterdam to Detroit with explosives hidden in his underwear, a man at Stuttgart airport made an unwise joke about a bomb – in his underpants. And even though, as reported by "Spiegel Online" on 5 January 2010, it later turned out that he was merely on his way to Egypt for vacation with his family and had no explosives or any other forbidden objects on him, he was detained by the Federal Police, subsequently missing his flight and facing a fine of up to 1.000 Euros.

We can in fact find liberal, yet highly regulative modes of governing airport security all around the world. While a great deal of research has almost naturally been concerned with changing regimes in the US, especially after 9/11, other parts of the world, mostly through regulations of international aviation organizations such as the International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO), have quickly attempted to harmonize their own modes of airport security. As Bærenholdt (2013: 27) points out, particularly "the *European Union* seeks to govern exactly *through* mobility in its endeavours to produce a frictionless space, overcoming missing links and promoting transnational activities in ways in which the networking and mobilities involved seem to become purposes themselves, if not, in fact the way power is mobilised in making European society and space [emph. in orig.]." Thus, mobility (and subsequently aviation) must not only be regarded as a technical means of movement, but also as constitutive of societies, of identities, and of spaces. Especially the latter notion of mobility as the production of space has more recently garnered increased interest from geographers who have engaged the spatial dimension of airports and their architectures and affects (Adey, 2008a; 2010; Bissell et al., 2012).

Liberal government at the airport in fact presents itself in manifold ways that resemble liberal economy. As Salter (2013: 9) compellingly summarizes the empirical situation, "the

contemporary mobility regime – with its various technologies of identification, examination, verification, and passage – functions in the same ways as the free market: a disaggregated system of controls for the movement of peoples does not guarantee any one outcome (and indeed guarantees mobility shortages just as the market guarantees shortages), but rather provides a structure in which certain outcomes are removed from the political realm and treated as either technical or economic questions." The rationale behind such a market approach, as indicated above, can arguably be best retraced through a Foucauldian account of biopolitical regimes. As Dean (2006: 15) puts it, "certain ways of governing, which we will broadly define as *liberal* modes of government, are distinguished by trying to work through the freedom or capacities of the governed [emph. in orig.]", and arguably the airport is very paradigm for such modes. Thus, how does airport security craft freedom against the backdrop of a seemingly restrictive agenda of control and inspection? The answer is rather simple: in liberal government as diagnosed by Foucault, freedom and security are not mutually exclusive concepts, but reinforce each other through population management. As he argues, "power is situated and exercised at the level of life, the species, the race, and the large-scale phenomena of population" (Foucault, 1984b: 260). Through a statistically empowered analysis of the population itself does security come into being, then.

If we create knowledge about the population, so the political argument goes, then we can exercise power in such fashion that the 'good' and productive parts of the population can be granted freedom (and subsequently unlimited mobility) while the 'bad' and disruptive parts must and can be excluded from mobility such that they cannot unfold any harm. As Foucault (2007: 64) frames the issue, we must think of "circulation in the very broad sense of movement, exchange, and contact, as form of dispersion, and also as form of distribution, the problem being: How should things circulate or not circulate?" It is the close proximity to the economy that is emblematic for the ways in which airports operate, and that has in fact centered around the question of how to empower and regulate flows of passengers at the same time. In Foucault's (2007: 65) terms, the task of government is then "no longer that of fixing and demarcating the territory, but of allowing circulations to take place, of controlling them, sifting the good and the bad, ensuring that things are always in movement, constantly moving around, continually going from one point to another, but in such a way that the inherent dangers of this circulation are canceled out."

In order to do just that, as has been outlined above, airports circle predominantly around the paradigms of surveillance and data gathering, such that from those digitalized streams knowledge can be created and eventually power can be exercised over flows of travelers. As Salter (2013: 10) points out, "practices of visas, preclearance, and electronic travel authorities/no fly lists, were in effect creating a globalized system for the surveillance of the mobile public", notably for the twisted sake of both freedom *and* restriction at the same time, divided among population categories of riskiness and trustworthiness. Such categorizations have been rendered the focal point for a politics of/at the airport. As Salter (2013: 10) adds, in fact "the global air network is essentially a slingshot orbit; good passports are like wheels; money is a near-universal lubricant, as well as social capital, race, language, etc.", and major public disputes have arisen from such categories that define the borderlines of social sorting.

Protests against invasive levels of airport security screening have reached such heights that in the US, in November 2010, an online community called 'We Won't Fly' (www.wewontfly.com) has formed that organizes nation-wide campaigns against the Transportation Security Administration (TSA) and its practices. Having originally emerged around doubts against body

scanners that featured 'naked images' of the human body at the time of roll-out, the community now more generally seeks to "catapult the cause of TSA abolition and the importance of human dignity and human rights (especially the 4th amendment) into the minds of hundreds of millions of people worldwide once again."

Arguably, the multiple techniques, technologies, discourses, and modes of governing that can be found empirically have rendered airports as such intriguing spaces for research. As Bærenholdt (2013: 22) claims, "the ways in which mobility is involved in the constant processes of redesigning and government of societies needs more attention", as, as Salter (2013: 15) adds, "the management of circulation is not consistent across time, space, or networks", and thus requires ongoing scholarly analyses. In fact, mobility politics must be understood as the all-encompassing attempt to digitally encode mobile populations in order to extract knowledge surplus from such data. As Dillon and Lobo-Guerrero (2008: 272) argue, such a biopolitical "grid of intelligibility is in short an accounting and valuing machine" that enables authorities to govern populations through risk, based on statistics. As has been shown throughout the narrative of security as future, the registers of risk themselves are manifold and transformative, and have historically centered around specific problems of governing. With the scope on mobile populations, a biopolitical mode of security adds another quickly transforming element to the equation. As Dillon and Lobo-Guerrero (2008: 283-4) explain, "biopolitical security discourses and techniques deal with an object that is continuously undergoing transformation and change through the manifold circuits of production and reproduction which comprise the very eventalness of its biological existence": the (mobile) population.

Multiple constellations of mobilities render airport security flexible such that it can be quickly re-adjusted according to the definition of new threats and/or political programs, but they also render airport security ultimately complex and academically challenging. We have to take into account the multiple modes of conducting "data derived from the intensification and extension of increasingly novel forms of counting, accounting and surveillance" (Dillon and Lobo-Guerrero, 2008: 277), as well as their future-related analytics that, depending on the modality of risk applied, may produce unstable and temporary social sorting through algorithmic techniques of data-mining, creating "mobile norms" (Amoore, 2011) for the adaptive regulation of mobility. A Foucauldian account of security highlights government as the management of de-territorialized, boundary-less and global flows of people and goods. Security, conceived through this lens, produces freedom and openness, and empowers modern economic principles, while at the same time shutting down those elements of the population that by specific discourses are rendered 'risky' and thus unwanted. The analytic pieces to follow attempt to unpack, or at least shed some light on some of those mechanisms, while at the same time accounting for their impact across the social dimension.

III. Analytics

"These pieces are written at that border between what one knows and what one thinks it might be possible to think, between what little one grasps and the great gulf of ignorance which that partial grasp reveals."

(Rose, 1999: 11)

Empirics

As has been indicated in the prelude, this PhD project evolved through the thematic layer of a research project (KRETA). Funded by the German Ministry of Education and Research (BMBF) and thematically focused on the multiple ethical, social, and political implications of body scanner technology, the project pursued a double approach of both empirical fieldwork and philosophical reflection. While conducting empirical research (ethnographic observations at the airport as well as a series of expert interviews with stakeholders from the aviation branch, broadly conceived), it quickly became clear that research on a specific security technology that was designed particularly for airport contexts could by no means stand on its own. As has been shown throughout the first two sections of this thesis, the notion of security is way too complex to be broken down to a mere, however multi-dimensional, analysis of checkpoint security and its transformation through a single technology. In order to do as much justice as possible to the myriads of notions and nuances of security, any analysis of airport security must thus proceed way beyond a single spatial and/or technological layer, and rather turn to a mode of problematization that incorporates the airport 'as-a-whole'.

This is why I decided to extend my PhD project beyond the rather narrow (however highly intriguing) scope on body scanners. Still, as can be witnessed by the empirical inquiries to follow, body scanners make an appearance as the main focus of analysis in two of the six pieces. [Inquiry 4] centers around the question whether body scanners can be conceived of as an attempt of securitization. The manuscript analyses the reasons why body scanner technology has not been implemented at German airports, unlike in other EU member states. Conceptualizing the struggle over the deployment of a new screening measure as a securitization process, the paper seeks to move beyond language and official discourse, in which the machines were framed as unsuitable in plain numeric terms. Sociological approaches to securitization theory thus can help to shift the scope to practices and expert knowledge in the aviation sector and to achieve a more profound understanding of securitization processes. Building on a series of expert interviews with representatives from relevant stakeholders, the piece argues that privacy requirements have created major obstacles for body scanner technology and finally contributed to the (preliminary) failure of a long-term securitization move. The analysis of body scanners as a thwarted securitization process obviously builds on the narrative of security as securitization, but it also explores some of the notions of security as technology and security as economy.

Body scanners are also the central building block in [Inquiry 2], co-authored with Anja Koenigseder, however from a much different, sociologically inspired angle. With the emergence of aviation as a target for terrorism and serious crime in the 1970s, the affective dimension of airport security changed drastically and is now carefully engineered as a zone of earnest and solemn protocol. Against the backdrop of bombings and hijackings, airport security today enacts a 'no bullshit' approach in the 'war on terror'. Humor essentially has been banned from screening operations. From obvious signs that say 'No bomb jokes, please' to drastic consequences in the case of non-compliance, security appears as something that is not to be fooled around with. However, with the introduction of body scanners at the airport, this atmosphere of earnest appears to change. The manuscript builds on ethnographic fieldwork at Hamburg airport during the German trial run with body scanners in 2011. During the time of observation, we found a surprising amount of reciprocal laughter and joking. We argue that this can be conceptualized as an attempt to break open a space for laughter, momentarily abandoning protocol in order to deal with issues of visualization, exposure and

shame that arise from the new scope on the fleshly anatomical body. The paper touches on the politicality of body scanners and more generally on the politics of counter-terrorism, but it takes a 'detour' through the sociality of technology. In this vein, the manuscript builds mainly on the narrative of security as (socio-technical) assemblage, but also on the narratives of security as technology and security as government.

Another empirical analysis that has directly emerged from the KRETA project is [Inquiry 5]. When analyzing the interview material, there was indeed a red thread throughout the transcripts that could hardly be missed: most of the experts at some point during the conversation highlighted the problematic state of security enactment on the ground level. In other words: they were concerned about the actual individuals who 'produce' security. Airport security both follows general trends of risk-based and technology-led policing, as well as it is determined by a neo-liberal economic mode of regulation, leading to privatization and out-contracting of most tasks, including actual screening of passengers at the checkpoint. The manuscript draws on those expert interviews from the aviation sector in order to scrutinize how German airport security governance can be located on the continuum between the public and the private. By combining both economic and political accounts of security, the analysis retraces how the particular German solution of a principal/agent relationship between the police and private firms remains stuck between a normative blueprint of state-provided security and the benefits of market regulation, and thus causes a series of problems. The manuscript is constructed around the narrative of security as government – more specifically: around the criminologically coined perspective of security governance – and draws a close link to the narrative of security as economy.

As mentioned earlier, the aim for this PhD project was to provide an analysis of security and the airport as encompassing as possible, and the empirical material from the KRETA project could only serve up to a certain point here. In order to create more accounts that provide further perspectives of how security comes into being in complex airport assemblages, I have sought to explore additional dimensions. Two of the analytic pieces that follow are particularly concerned with the notion of "social sorting" (Lyon, 2003d). [Inquiry 1] evolves around a presumed conflict between risk and privacy, and the cross-cutting practices of data collection we find at the airport. Risk has become a ubiquitous tool for security governance. The manuscript analyzes the ongoing shift in airport/aviation security from rule-based to risk-based screening. Seeking to explore the effects of data based passenger risk assessment on privacy through the collection and processing of personal data, the paper argues that risk is likely to enroll passengers into a partly voluntary, partly enforced membership in trusted traveler schemes in order to enhance the database, thus enabling a more precise assessment of risk levels. In a disciplinary spatial setting, the once distinct privacy dimensions of citizen-state and consumer-market become increasingly blurred, as law enforcement authorities seek to exploit data that was originally obtained for commercial purposes to improve risk calculations. The manuscript strongly builds on the narrative of security as surveillance, and on the underlying narrative of security as future.

The notion of security as future is in fact one that has particularly fascinated me, and [Inquiry 6] further explores the political modes of addressing the future at the airport. The paper argues that with increasingly large databases and computational power, profiling as a key part of security governance experiences major changes. Targeting mobile populations in order to enact security via controlling and sifting the good from the bad, profiling techniques accumulate and process personal data. However, as advanced algorithmic analytics enable

authorities to make sense of unprecedented amounts of information and derive patterns in a data-driven fashion, the procedures that bring risk into being increasingly differ from traditional profiling. While several scholars have dealt with the consequences of black-boxed and invisible algorithmic analytics in terms of privacy and data protection, the manuscript engages the effects of knowledge-generating algorithms on anti-discriminatory safeguards. Using the European level efforts for the establishment of a Passenger-Name-Record (PNR) system as an example, and on the theoretical level connecting distinct modes of profiling with Foucauldian thought on governing, the paper finds that with pattern-based categorizations in data-driven profiling, safeguards such as the Charter of Fundamental Rights of the European Union or the EU data protection framework essentially lose their applicability, expressing a diminishing role of the tools of the anti-discrimination framework. Besides its strong focus on the narrative of security as future, the manuscript also explores the narratives of security as surveillance and security as government and re-connects them to the narrative of security as value.

The last empirical inquiry occupies a special position among the array of manuscripts on airport security. It is not directly concerned with aviation, but with the complex relation of security, technology, the industry, and the field of security research. As already indicated in the prelude, I have opted to incorporate questions of security research as part of the political program of security, as they have strong relevance for more general questions of the social, political, and economic role of security. [Inquiry 3] thus engages the storied relation of security and privacy and its transformations through the layer of security research. Privacy and security have long been framed as incommensurable concepts that had to be traded off against each other. While such a notion is rather under-complex, it has been quite persistent. In recent years, however, the relation has undergone a transformation and is now apparently conceived of as a technological issue that is set to be resolved through privacy by design. The manuscript retraces, through an analysis of EU security research funding, how this shift has come about, and critically assesses its potential to eventually resolve the conflict between privacy and security in a world of data-driven security measures. Thereby, it builds on the narratives of security as transformation and security as technology, and links them closely to the narrative of security as economy.

Besides highlighting specific registers of security individually, one common narrative that all inquiries touch upon is the initial one that has briefly explored security as value. They all raise normative questions, often from a critical standpoint that seeks to challenge the modes in which security is used as a means of re-ordering the social through distinct modes and rationalities of government. Particularly, they emphasize the colonization of the everyday which has become so crucial for a critical security studies agenda. The inquiries understand themselves as deeply indebted to, as Bigo (2008a: 16) frames it, “a political sociology of international relations that reintroduces international phenomena, by making them normal and banal social facts on a daily basis” and renders them challengeable through academic analysis. Quite naturally, as a researcher based in Germany and funded through both German and European security research frameworks, their main scope is the European Union – however without being geographically limited in the arguments they put forward. As has been shown, an analysis of mobility is by default an analysis that incorporates a global perspective. As people, goods, and services travel, so do insights about the regimes that monitor and regulate such travel. The analytical inquiries presented here are at different points in their path of flight towards publication, as respectively indicated. They are presented in the form of finalized manuscripts.

[Inquiry 1]

Blurring the dimensions of privacy? Law enforcement and trusted traveler programs

On 27 September 2011, the European Commission held a High Level Conference in Brussels on "Protecting Civil Aviation Against Terrorism." In the final document, the experts from Europe, partnering countries and the International Civil Aviation Organization (ICAO) recommended that aviation should turn to a more risk-based policy, stating that "security measures can and should relate to the risk they intend to mitigate" (European Commission, 2011c). The conference was followed up by another High Level Conference, this time held by the ICAO itself, that assembled more than 700 international representatives in Montréal, 12-14 September 2012. In its final communiqué, the conference "encouraged ICAO Member States and industry stakeholders to adopt a risk-based approach to aviation security" (ICAO, 2012: 2). Those are two striking examples of a security policy shift within an area that is considered both as highly symbolic and vulnerable, and thus has served as a prime target for any terrorist and/or criminal attempts. This paper seeks to explore the effects of this turn to risk as a key tool in the 'war on terror' on privacy in aviation. Theorizing the efforts as security governance (Wood and Dupont, 2006a), it will be shown how dispersed actors converge in their desire to create transparent individuals, using trusted traveler schemes as incentives, as they promise both rewards and the possibility to circumvent invasive secondary screening measures for passengers. Considering the contextual peculiarities for privacy (Nissenbaum, 2010) at the airport, it will be argued that individuals have little leverage in negotiating privacy boundaries, but are 'softly forced' into participation in trusted traveler programs.

The strong emphasis on risk in debates about aviation security has arguably emerged in a period of time when the cross-pressures on stakeholders have become more severe. In recent years, in addition to pressing security needs in the 'war on terror', aviation has faced rising numbers of overall flights and passengers and the need to work even more cost-effectively, while still providing maximum passenger convenience. At the intersection of these cross-pressures lies passenger screening at the airport, where in a spatial bottle-neck security becomes enacted through the evaluation of whether the passenger poses a threat or not. Modern airports have been stacked with a variety of security and surveillance measures for a long time, ultimately culminating in intense screening procedures at the checkpoint that separates the publicly accessible landside area and the secured and 'sterile' zone of the airside area. Security screening has traditionally been carried out based on a principle of equality, meaning that everyone has to be screened with the same intensity. A simple problem has been identified within this current approach to airport security though, which is nonetheless hard to overcome. Past implementations of security measures and technologies in screening can be understood as a causal chain of incident and reaction – either in form of policy change or in form of new technological measures. Among the most prominent and controversially discussed examples of this sequential logic are the ban of liquids and the implementation of whole body imaging devices ('body scanners'). However, there has been considerable critique towards such a reactive approach to airport security. The layering of security policies and measures at the checkpoint leads to "large increases in costs and inconvenience to travelers with a small corresponding increase in security" (McLay et al., 2006: 333), "but still [does] not manage to capture a clever and adaptive adversary" (European Commission, 2011c). Or, as Jackson, Chan and LaTourrette (2012: 1-2) have put it: "Questions have been raised about the basic philosophy of aviation security, which is that security is applied uniformly to all." Thus,

aviation experts have deemed risk as a convenient and powerful remedy to the multiple concerns in aviation security. Airports appear to be a perfect fit for risk management strategies, since security screening channels large and mobile populations into a neat spatial setup in which security managers strive to examine the individual carefully. As Jones (2009) has noted, security mechanisms at the airport essentially come down to the checkpoint as the single valve that ensures the integrity of the secured sectors and prevents security breaches via the ability to stop and to sort out. Hence, in aviation's struggles in the 'war on terror', the screening checkpoint can be considered the key tool against high-jackings, bombings, and whatever other worst-case scenarios security managers have mapped out as possible events.

Along with the introduction of risk, considerable change is coming to the checkpoint. Where in the past a rule-based or bureaucratic paradigm (O'Malley, 2006) prevailed, new concepts for future screening are taking up the notion of increased distinction based on risk categories and intend to introduce mechanisms for an a priori analysis and sorting of passengers, enabling airport authorities to either add or subtract layers of security measures, according to the assigned risk level of a given individual. At its 2011 conference in Singapore, the International Air Transport Association (IATA, 2011) has presented a concept for the 'Checkpoint of the Future'. Much like the US CAPPS II system that intended to compute statistical risk estimates for each passenger (Barnett, 2004: 912), the IATA concept is set to collect and process as much passenger information as can be made available. While CAPPS II had been "eventually dismantled over privacy concerns" (McLay et al., 2006: 334), the IATA concept still intends to link multiple data sources, both from the public and the private sector. The risk estimation model is supposed to be supported by passenger data, trusted traveler databases, behavior analysis, and biometric identity management (IATA, 2011: 6). Travelers would then be screened on different levels of intensity, depending on their assigned risk level. A very similar approach is being pursued in a joint effort by the Airports Council International (ACI) and the Association of European Airlines (AEA). Their 'Better Security' concept states that "with greater focus on intelligence-based security, passenger name record (PNR) data has increasingly come under the spotlight" (ACI/AEA, 2011), and thus suggests that "closer international co-operation and data sharing should be used to strengthen the effectiveness of passenger profiling, flagging suspicious individuals" (ACI/AEA, 2011).

Within the multiplicity of identified data sources, the inclusion of trusted or registered traveler programs seems most notably unique, for it is based on voluntary participation. Passenger information is usually being obtained by airlines for commercial purposes in the form of 'Passenger Name Record' (PNR) or 'Advance Passenger Information' (API) files. While the latter contains only information about the individual's identity and passport documents as well as the travel itinerary, PNR goes beyond that basic data and contains also the likes of contact and payment information, including credit card number, baggage details, the traveler status and even special dietary requirements on the flight. Thus, PNR data has been turned into an asset for security operations by the US Department of Homeland Security (DHS) via the 2007 EU-US PNR Treaty. Also, other forms of information gathering like behavior analysis and identity management (either biometric or conventional) may not be circumvented by the passenger. Data sources in risk-based passenger screening might thus be divided into 'no opt-outs' and 'opt-ins', with trusted traveler information being the only source that passengers can opt-in to. Or, as the IATA concept states: "Further assessment can be made through passengers voluntarily providing more information about themselves, through known traveler programs" (IATA, 2011). According to Jackson, Chan, and LaTourrette (2012: 2), successful passenger differentiation can be achieved via the identification of individuals who pose more

risk or via the identification of individuals who pose less risk to aviation. While the former is based on the 'unknowns' about the individual in question, the latter form is concerned with what is already known about a passenger and how that information can be exploited in order to determine the individual's trustworthiness. "Trusted traveler status allows these passengers then to go through less-intense screening than would have been the case without the program, and the remainder of the public receives more intense screening" (Jackson et al., 2012: 3), effectively establishing both a re-allocation of scarce economic resources and providing increased customer convenience for 'trusted' travelers. Framed as a form of panacea by aviation security practitioners, the inclusion of trusted traveler data thus facilitates screening and provides incentives for the participation in the programs at the same time.

Exploring the possibilities of added information sources in terms of trusted traveler status, the EU Commission Directorate-General Energy & Transport has issued a study on the feasibility of registered passenger concepts in order to "whether such passengers could be exempted from certain controls without compromising security" (Accenture, 2007: 2), coming to the conclusion that "the information submitted by a passenger for enrollment into an RP scheme may enable a 'not high-risk' judgement" (Accenture, 2007: 3). But at the same time, the authors recognize that clearance in terms of trustworthiness does not eliminate the risk that known travelers might be 'sleepers', or that they might be coerced or duped into terrorist attempts (Accenture, 2007: 3), thus claiming that trusted travelers essentially could not be screened with less intensity. However, analyzing a number of existing trusted traveler schemes, including well-known programs like PRIVIUM, NEXUS, IRIS or CanPASS, the report finds that screening and access to the checkpoint could at least be facilitated and accelerated (Accenture, 2007: 9). As for concepts like the "Checkpoint of the Future" and "Better Security", trusted traveler programs would remain but one of several indicators for risk assessment, among other information sources including flight route and type, passenger data, double-checks against government databases like terrorism black lists or no-fly lists, biometric identity management and behavioral analysis (IATA, 2011: 11). Nonetheless, trusted traveler data is being pursued as a valuable additional data source for risk management.

Security, risk, and privacy

This tendency falls in line with what has been deemed as anticipatory post-9/11 policy turn, enacting precaution and preemption based on a "quasi-permanent state of exception" (Tsoukala, 2010: 41). A common ground that can be observed in all of the official documents is the strong emphasis on the collection of data, and, more importantly, the convergence of databases. The aviation sector thus envisions international standards of data sharing and interoperability, paired with mutual recognition of risk assessments (IATA, 2011). In order to understand the hunger for comprehensive data on individuals in aviation security, one has to look closer into the concept of risk. The scope on data at the airport enacts a form of "surveillant assemblage" (Haggerty and Ericson, 2000), encoding the individual into digital information profiles. Those mechanisms have empowered the turn from traditional surveillance to "dataveillance" (Amoore and de Goede, 2005), enabling authorities to govern populations based on the available individual information. The crucial assumption of risk is that uncertain futures could be rationalized and then managed, treating risk factors like business assets. In screening, this claim comes into being via individualized risk assessment, based on knowledge in the form of passenger data. Statistical risk assessment is realized via the collection, linkage, processing and finally evaluation of a sufficiently large database.

Featuring a clear scope on passenger information, practices of data collection and sharing in aviation have repeatedly drawn the attention of privacy researchers (see for instance Bennett, 2005; 2008). Arguably, risk assessment is adding a new dimension of quality to data based surveillance and possible social sorting. It becomes clear then that in terms of privacy impact assessment, risk-based screening at the airport has to be scrutinized carefully.

Starting from the notion that "privacy is a moving target" (Friedewald et al., 2010: 61), it should briefly be clarified how the concept can serve as an analytical tool for data handling practices at the airport. The buzzing debates on concepts, regimes and policies of privacy, including a lot of critique towards the concept of privacy as an adequate toolbox in the first place, have been reflected in Solove's (2008: 171-2) somewhat cynic remark that privacy may very well serve as a generic term for a whole cluster of problems that need not necessarily be located along the same dimensions and therefore share not much but the lack of a common denominator. Nonetheless, privacy (along with the concept of data protection) has become one of the catchphrases in public debates when it comes to defending civil liberties against whatever form of surveillance and control measures they would be endangered by in the name of security. Today, most scholars have abandoned the classical paradigm of privacy as "the right to be let alone", as it had been proclaimed by Warren and Brandeis (1890) more than a hundred years ago. However, there are still approaches that tend to reproduce a perspective that carries a somewhat individual-centric notion and emphasizes the control that individuals should possess over their personal data. That is, for instance, to whom information would be communicated, at which point in time, and to what extent (Westin, 1970). This kind of understanding remains within the spatial assumption that privacy should be considered as some kind of bubble around the individual that has to be protected from intrusion and pairs very well with the often proclaimed notion that privacy would be the counterpart to modern surveillance (for a contest of this relationship, see Gilliom, 2011).

Concepts that solely remain on the individual level arguably neglect a broader societal perspective, though. Several scholars have put an emphasis on the fact that privacy must be regarded as a common good as well, that might be balanced against other values (Friedewald et al., 2010: 61). Drawing on Altman (1977), Steeves (2009) has pointed out that privacy in modern societies should be analyzed as a dynamic process that is constantly involved in negotiating personal boundaries. Building on that argument, Nissenbaum (2010) has made a significant impact on the debates with her notion of context related concepts of privacy. Both boundaries and contexts then would not only consider other individuals, but organizations and institutions as well (Bennett, 2011: 489). As in the case of passenger screening, it might very well be argued that individual claims of privacy are prone to be overpowered by the common good of security, and that passengers should be willing to accept certain cutbacks in privacy in order to guarantee the higher value of shared security for all. Considering that the framing of contemporary security as a means to grant protection from a ubiquitous terrorist threat has become the defining paradigm for shaping concrete security frameworks, the position of privacy claims arguably becomes weakened. Security discursively seems to trump individual as well as societal privacy. Along these lines, Stalder (2011) has pointed out that in numerous situations in everyday life, individuals have to provide personal information against their will, and have little or no bargaining power. Considering future-related governance, it is not so much security itself that poses a threat to privacy, but the notion of risk and the claim to calculate the probability of future events, based on individual data.

Thinking privacy in terms of contextuality, an analysis of aviation security poses some major hurdles in terms of the fragmented nature of the topic. Being an international matter that is regulated through an assemblage of international organizations, national regulations and bilateral treaties, overlapping or unclear legal frameworks of privacy and data protection might well be the case, as has for instance become obvious in the EU-US PNR debates. While in the EU passenger information is protected by the European data protection framework (Official Journal of the European Communities, 1995), the same data when transmitted to the US underlies distinct legal regulations. Moreover, airports themselves depict a prime example of spaces where individuals possess little to none leverage when facing screening and the conduct of personal information. Thus, possible negotiations of privacy boundaries are being suppressed in the first place. In order to assess the impact of recent developments in aviation security, it is important to analyze how risk is brought into being at the airport and how it impacts privacy. Or, put more precisely: the analysis will be focused on the way how privacy 'negotiations' are affected by the notion of risk assessment and management, eventually leading to a situation in which fair bargain becomes blocked, since too much is at stake for the passenger. A refusal of information disclosure rules out the possibility to fly and essentially hinders any rational forms of resistance against data processing practices of airport authorities. On the contrary, taking up Westin's (2003) thesis of distinct privacy dimensions, it will be shown that with the inclusion of trusted traveler schemes, the dimensions of privacy become increasingly blurred, illustrating a larger trend in which "the application of risk techniques in the war on terror fosters complex new spaces of governing in which public and private authorities, knowledges and datasets cooperate closely, and sometimes become practically indistinguishable" (Amoore and de Goede, 2005: 7). Not only do law enforcement authorities seek to exploit commercial databases, but moreover can the membership in trusted traveler programs potentially contribute to the assignment of a low-risk status, skewing the inconveniences in screening towards the less mobile and economically disadvantaged parts of the population, and leading to increased "self-governance" (Amoore and de Goede, 2005) of the passenger, who becomes likely to voluntarily disclose additional personal information in background checks for the sake of less distressing travel.

From security governance to risk governance?

Theorizing aviation security as governance makes it possible to turn the attention to the dispersed network of actors through which it becomes enacted (Yar, 2011). Emphasizing the achievement of desired steering effects as a result from multi-party networks including public as well as private sector agencies, Rhodes (2007) provides a pragmatic approach to the analysis of governance. However, several authors (Loader and Walker, 2006; Zedner, 2007) have pointed out that the diminishing role of the state in governance creates problems in terms of accountability, legitimacy and social justice when it comes to the provision and distribution of security. With the rise of risk, those problems arguably become amplified. While in economic contexts risk is often framed as an opportunity, more often the term bears a negative connotation. Risk is the probability of something happening, and while it can be argued that making a risky investment can indeed turn into a chance, the notion of risk as future harm overwhelms in security discourses. Risk then intuitively becomes connected to accident, crisis, emergency, catastrophe, or disaster. Thus, the assessment and management of risk intends to tame the possibility of harm. In the governance of mobile populations, risky elements are to be sorted out of the flow in order to prevent devastating events such as 9/11.

Risk assessment quantifies the chances that the future will indeed go wrong and that the state of normalcy will collapse into a chain of events that contests the ritual and breaks the habit. Following this logic, risk is both an indicator of the possibility of future events as well as a factor that should be minimized by establishing precautionary counter-measures.

Paving the way for a social science analysis of risk, Beck (1986) has introduced his interpretation of the "risk society", hinting at the ubiquitous use of the concept of risk in numerous areas of contemporary societies. Put briefly, risk appears as a way to cope with the unknown structures of the future by capturing its temporal dimension and relating it back to the present, where it can be dealt with in terms of management, mitigation, reduction or even avoidance. However, considering the fact that the unpredictability of terrorism exceeds the claim of control in terms of management, Beck comes to the conclusion that risk as a policy tool can merely "feign control over the uncontrollable" (Beck, 2002: 41). Despite this logical flaw, risk has increasingly found use in security governance, enabling policy makers to enact a pro-active role and to shape security in the name of precaution, thus acting upon an identified threat before it reaches the point of irreversibility (Anderson, 2010a). In the statistical turn towards probabilistic thinking, risk promises to grasp uncertainties and to convert them to plain numbers – which would then be easy to interpret, easy to understand across cultural and linguistic borders (Hansen and Porter, 2012), and, maybe most importantly, easy to use as an argumentative basis for policy makers to establish security measures that would reduce the likelihood of occurrence of future harm.

As a most welcome side-effect in trying to tame the uncertainty that is "the basic condition of human knowledge" (Ericson, 2006: 346), the contemporary deployment of risk management promises to soothe some pressing concerns in times of scarce resources, thus introducing a notion of economic benefit into the management of future contingencies. With security governance in aviation increasingly becoming risk governance, the assessment of risky individuals is set to provide a support for decision-making on where to allocate limited resources in order to achieve desired policy outcomes in the most effective way. This rationale enables airport authorities to subtract or add screening measures in order to increase both speed and passenger convenience level at the checkpoint. The question whether the concept of risk really transfers to the social level constantly lingers over the debates on risk regimes, and has been deemed controversial (Aradau et al., 2008; Manning, 2006; Tsoukala, 2010) as it neglects the concept of free will and the unpredictability of human behavior. Risk in terms of precautionary politics means thinking about the intentions of individuals, based on available criteria and large amounts of data that are being put into predictive models (O'Malley, 2004: 1). In this attempt to rationalize human behavior, "technologies of risk management provide a logical connector for developments which seem to lack a common rationality", as Aradau and van Munster (2007: 107) have noted, hinting at the sometimes arbitrary establishment of a causal chain between indicator variables and estimated risk level. The analysis and management of risk originally stem from environments that feature physical and material sequences in material environments, such as engineering or statistics, and arguably this is the area in which they work best (Manning, 2006: 455). For in those environments, all relevant variables and indicators for risk estimation are known and models can be designed adequately, so that calculated estimates can be considered robust. However, with regard to social and individual behavior, risk profiling can merely serve as a proxy for real evidence (Cavusoglu et al., 2010: 1288).

Empirically, the application of risk can be found in various political and social areas, including fields such as insurance, health care, the financial system and border control (Amoore and de Goede, 2005: 149). Especially in the security sector, the problem of contingency and the 'war on terror' has been increasingly framed as a matter of risk management, thus contributing to the deployment of risk assessment in several contexts, most visibly at symbolic sites like airports and the border. As O'Malley (2004: 1) has drastically put it, risk-based routines and practices dominate many aspects of contemporary life, establishing a form of governance that not only targets, but also incorporates individuals and turns them into everyday risk managers themselves. Thus, risk seems to have colonized the state of normalcy (Aradau et al., 2008: 154) in the name of the 'war on terror', reminding of what Agamben (2005) has tagged as the "permanent state of exception", and putting security governance into the realm of emergency and urgency. Ultimately then, security governance shifts to risk governance.

If this is true for society in general, it is particularly true for aviation. Extreme events like 9/11 and the terrorist bombings in Madrid and London have painfully emphasized the vulnerability of the transportation infrastructure that supports liberal ways of life. Dealing with events of low probability but high impact, security policy makers felt the urge to find a way to deal with catastrophe, disaster, and emergency on a basis that was suitable for governing the future from within the present and to establish a maximum of both precaution and on the other hand preparedness for the worst-case. Consequently then, in the wake of 9/11, security policy was predominantly framed as a problem of risk management (Amoore, 2006: 337). International aviation, as the entrance point for the terrorists of 9/11 and highly symbolic for the use of aircraft for the attacks as well as for its promise of free and fast global movement, has arguably undergone the most enduring effects in terms of changing security regimes since then. Yet, as Jacobson (2012: 35) states, the aviation system today is at its most risky point since 9/11, still focusing on objects as material threats and introducing security measures and policies only as ex-post reactions to incidents like the 2001 shoe bomber, the 2006 liquid explosives plot or the 2009 underpants bomber (Jacobson, 2012: 36). The awareness of this problematic backwards approach that looks into past events in order to adapt the present has arguably fostered the turn to risk. Looking into the future, risk has to rely on predictions about the intentions of individuals, whose actions then might eventually materialize as worst-case events such as terrorist attacks. The focus thus shifts from the concrete to the vague, from situational crime prevention to full range surveillance of individuals and personal data.

Risk governance aims at replacing subjective anticipations of the future with standardized equations which provide an outcome of most precise predictions. Or, in other words: risk assessment is the attempt to transform fluid uncertainties into calculable terms, based on 'hard' facts in terms of passenger information. It thus represents a rationalized form of thinking that moves away from subjective evaluations and estimations of the unknowable, and strives to establish the possibility to govern the future, based on numbers. For this purpose, managers of risk attempt to encode individuals into categories of riskiness, separating the trustworthy and legitimate from the dangerous and illegitimate parts of the population (de Goede, 2008a: 158). Thus, risk has been tagged as an instrument for governing the social (Aradau and van Munster, 2007: 91) by putting populations "at risk" (Aradau et al., 2008: 151). Exposing passengers to scrutiny and categorization, it becomes possible to sort populations, identifying and acknowledging the 'good' parts, while exercising restrictions on the 'unwanted' parts, as has repeatedly been stated with regards to border control regimes and practices (see for instance Amoore, 2006; Bigo, 2001; Epstein, 2007; Lahav, 2008; Muller, 2009; Pallitto and Heyman, 2008; Salter, 2004). Airport screening increasingly draws on the

same patterns, setting up a mechanism that resembles Bigo's (2001) figure of the Möbius ribbon that identifies high-risk outsiders from the inside of the population of passengers. As opposed to border control and immigration, risk assessment at the airport does not come into being on the basis of nationalities and passports, but on the grounds of passenger information. Lyon (2006a) has described airport security as a mechanism of social sorting, enacting dataveillance as "routine and focused attention to personal details for the purpose of influence, management, care, and control" (Lyon, 2006a: 403). Checkpoint security traditionally has worked as a stand-alone measure (Jones, 2009: 98), but becomes increasingly linked to data-based risk assessment, providing tools that serve as decision support systems that complement technologies of situational crime prevention with indications on where to intensify scrutiny and where the screening might be reduced on the basis of an established trustworthiness.

Context: disciplinary spaces

As well as in case of privacy, the meaning of risk may also vary considerably, and depends on disciplinary contexts and concrete settings (Zedner, 2006b: 424). The major stake for security regimes is how to govern large and mobile populations (Martin and Simon, 2008: 287), which means that for the sake of managing risks, individual behavior becomes encoded in the data structure. At the airport, those data are being provided through "routine procedures of classification and categorization" (Aradau et al., 2008: 149) in the form of PNR/API and trusted traveler schemes, verified by (biometric) identity management and double-checked against remote databases, enacting aviation's focus on identity and the gathering of data (Jacobson, 2012: 37). As Adey (2008b: 146) notes, being "symbols of the securitization of public space, airports employ the latest surveillance techniques in order to identify and target terrorists, threats, or risks." The ever-increasing desire to conduct as much information as possible in order to complete the basis for risk assessment appears to be a ticking-bomb-scenario in terms of civil liberties and human rights in general (Tsoukala, 2010; Zedner, 2006b: 425). Thinking about recent developments from a privacy perspective, surprisingly little resistance has manifested against data collection and data exploitation in risk governance. Especially practices in transportation security seem to be well tolerated when compared to commercial private sector operations. This lack of resistance is hard to retrace when taking into account that the majority of passenger information is collected and/or handled by private companies.

In the commercial sector, more and more companies have mastered the challenge of providing custom-tailored and personalized services (Stalder, 2011: 510). Global trailblazers like Google, Amazon or Facebook, to name some of the most prominent examples, proudly announce that each of their users/customers will face different and individualized treatment, depending on their needs and wishes. But this modern promise has kindled an intense debate on practices of data-mining, thus raising public awareness towards the collection, storage, and analysis of personal information by private companies. While in a liberal market environment, it seems comparably easy to perform an opt-out from such practices and to choose another (digital) shopping venue, a different provider, or to abandon membership in social networks, the situation at the airport is a very much distinct one. Screening in aviation security fundamentally differs from free choice. Passengers are not entitled to opt out from screening, unless they would accept to stay grounded after all. It has been argued that in aviation, a business relation between customer and carrier airline is being established by purchasing a ticket and accepting the terms of business. But flying is arguably more than just business.

Besides being symbolic and part of the contemporary paradigm of mobility, aviation is a highly relevant area for national and international security, which is why usually public authorities and/or law enforcement are involved in security screening at the airport.

Thus, the individual's surrender to risk assessment and the disclosure of personal data becomes mandatory, whether or not this might be accompanied by major privacy concerns. The lack of resistance has partly been ascribed to an environment that is as intimidating as an airport in the first place. Airports have been deemed as places of extreme discipline (Lyon, 2003a), where privacy-invading security measures were more likely to be accepted than elsewhere. This might partially be based on fears of terrorist attacks, but also on the 'liquid' characteristics of the airport, often compared to what Augé (2006) has deemed as modern "non-places" that only exist for the single purpose of transportation and feature a lack of permanent inhabitants and regular social interaction. In places of mobility, where everybody essentially remains a stranger to everybody else and travelers are constantly on the move, no traditional social mechanisms like trust between individuals can be built and established in the short period of time that a traveler spends at a transportation hub (Hansen and Porter, 2012: 415). Thus, to be able to assess who poses a threat and who can be rendered harmless, knowledge about the travelers has to be created. Drawing on Haggerty and Ericson (2000), risk assessment in screening tackles security concerns via the creation of "data doubles." Passengers become enrolled in a regime that operates on the basis of virtualized characteristics, encoding individuals into algorithmic risk calculation.

The lack of resistance against privacy infringements might also be due to the invisible setup of data collection for risk governance. Only with the inclusion of opt-in trusted traveler schemes, the disclosure of personal information re-enters the sphere of public awareness. And, unlike accepting the terms of business with the purchase of an airline ticket, the enrollment in a trusted traveler program requires pro-active individual initiative. So, on the one hand, it could be argued that informed consent is more likely in this case, but on the other hand, practices of data processing and transfer still remain opaque. The use of trusted traveler data, as it has been proposed by the IATA and ACI/AEA in order to expand the database for risk assessment, features additional caveats. Trusted traveler programs today appear on a global level and in a multiplicity of forms that require distinct forms of registration, background checks, disclosed information, membership fee and benefits. This variety is due to different scopes, among others on border control, immigration, the coverage of complete individual journey trails or simple customer convenience (Accenture, 2007: 11), complicating the choice of an adequate analytical level.

The US based Global Entry program, for instance, requires a profound background check which is being supported by an interview with a US Customs and Border Protection officer in order to approve of the applicant's low risk status. If this application is deemed successful, biometric identifiers are collected for the purpose of identity management at the airport. Global Entry currently is available for US citizens and legal residents, as well as for citizens of the Netherlands, South Korea, and Mexico, via bilateral treaties that regulate the exchange of passenger information between the participating countries. For instance, the bilateral treaty between the US and the Netherlands is coordinated by the so-called FLUX (Fast Low Risk Universal Crossing) Alliance. Accordingly, Schiphol airport in Amsterdam, being one of the major hubs in Europe, offers the use of the Dutch PRIVIUM program as equivalent to Global Entry. Focused on border control and immigration processes as well, the PRIVIUM scheme also features a scope on passenger conveniences and provides access to lounges, valet

parking, shopping discounts, airport assistance, and the use of exclusive fast lanes for an accelerated access to security screening. Besides the collection of biometric identifiers, enrollment into the FLUX Alliance requires the disclosure of full employment record for the past five years in addition to the membership fee for the PRIVIUM scheme. Being used in advertisement as a unique selling point, biometric identity management is offered in form of the possibility to accelerate border crossing by providing an iris scan to an automated kiosk instead of queuing up and showing ID documents to a border officer.

The use of technological advances like, in this case, iris recognition, is part of what has been identified as part of a PR strategy within aviation (Accenture, 2007: 8), demonstrating to the public that airlines as well as airport operators are pursuing pro-active strategies to make aviation more secure. And although the use of the advanced features requires the collection of biometric data, which can be considered as highly sensitive personal information, especially frequent fliers seem to be intrigued by the time-saving opportunities, combined with preferred treatment and 'cool' and 'futuristic' gadgets, making them part of an avant-garde global elite. Another example from the non-western context can be found in Dubai and Abu Dhabi. At Dubai International Airports, frequent fliers are offered the possibility to apply for an eGate Card, which is issued by the General Directorate of Residency and Foreigners Affairs. Eligible for Dubai citizens and ex-patriates with a visa, the card holder becomes entitled to circumvent immigration procedures by simply swiping the card through a card reader at an automated kiosk and confirm with his or her fingerprint. For a membership fee of about 40 EUR (200 AED), the registered and thus 'trusted' traveler receives a smart card that features an RFID chip, while the submitted data (passport, photo, finger print) becomes stored in a central database. The Dubai government advertises that entering and exiting the country would be possible in about 5-10 seconds when using the eGate system.

From an industry point of view, the establishment of trusted traveler programs is indeed a crafty move, since they provide multiple advantages for aviation security stakeholders. First of all, through membership fees, revenue is generated, which might not make the programs cost-neutral, but which at least contributes to an efficient implementation. The second advantage, as already discussed, is the passenger's voluntary disclosure of additional personal information, either in standardized form or in profound background checks, including interviews with the applicant and their family and close friends, as well as biographic data and biometric identifiers. The third move is the enrollment of the trusted traveler into a form of self-governance regime, expecting the passengers to handle security issues and other checks and screenings themselves. Contrary to the automatic and "hidden" (Bellanova and Duez, 2012: 122) collection of passenger information in PNR and API files and double-checks against remote databases, trusted traveler programs bring the disclosure of data back into the sphere of visibility and individual awareness. There is nothing obscure or opaque about membership requirements in terms of additional information and background checks – it might even be argued that the enrollment into trusted traveler schemes represents a form of informed consent. Since it could be assumed that the status as a trusted traveler is something that is desired and which advantages and disadvantages might have been weighed against each other, passengers would simply 'pay' for low-risk status with their personal information.

But such an argument appears flawed. As has been discussed, the disciplinary setup of airports does not allow for a real negotiation of privacy boundaries. Aviation security is a field in which recent developments have shown that risk-based policies do not only seek to identify risky individuals, but also seek to offer less intense screening to known travelers, for a number of

economic reasons. As Poole (2009: 101) puts it, there would be three distinct categories of passengers, based on the authorities' knowledge about the individual. Besides the regular traveler, there would be the low-risk passenger, about whom sufficient information would be available to execute an extensive risk assessment (with a positive result). The high-risk category, on the other hand, would be characterized by either negative knowledge, or, more importantly, the lack of knowledge. This would then include individuals "with no paper trail" (Poole, 2009: 101), thus passengers with an airline ticket that was bought by cash or passengers who previously never entered a given country via an airport. In risk-based security governance, not being known to public authorities represents a form of threat that can be compared to what Amoore and de Goede (2005: 158) have identified as the increasingly suspicious notion of cash money in the international financial system. As they note, "the world economy is a deliberately open and porous one, designed to encourage the free flow of capital, investment and economic development" (Amoore and de Goede, 2005: 153). In a similar fashion, aviation enables the free movement of individuals and goods. But only what can be surveilled, traced, calculated, assessed and managed appears to be trustworthy. The conflict between privacy and security found here is indeed a serious one. As security is being enacted via the concept of risk, the relationship between security governance and privacy is growing even more tense, as risk seeks to translate personal information into security assets.

Thinking about contextual integrity, aviation security policy turns into a mechanism of information-production. As Salter (2007) notes, airports enforce the surrender to a "confessionary complex", which with the rise of risk is being further amplified. The exploitation of trusted traveler data only seemingly turns the power relations between passenger and security screening upside down. Offering the possibility to circumvent some invasive screening measures, the individual is free to do so by enrolling into one of the numerous public-private partnership programs, thus arguably regaining some of the lost ground in privacy negotiations. Only that there is no ground to be gained in terms of privacy, but only in terms of less distressing screening. Or, in other words: the paying customer who abandons privacy concerns and offers full surrender of personal information receives double benefits from the private economy and from law enforcement. For the multiple stakeholders in aviation, such a symbiotic relationship generates a number of advantages. Airlines would become enabled to enhance customer convenience and airport authorities might speed up screening operations, from which also airport operators could profit, as travelers could spend the saved time to explore the airside shopping opportunities. Lyon (2003a) has in fact foretold an increased convergence of once separated surveillance systems from private economy and law enforcement in the follow-up of 9/11. Several scholars have since then pointed out that contemporary security governance in transportation and mobility is indeed structured as a "decentralized, rhizomic system of surveillance, in which travelers are constructed as manipulable entries in remote databases" (Lyon, 2003a: 15).

Bennett (2005; 2008), for instance, has analyzed the cascade effects of data collection, analysis and sharing that become triggered by the mere purchase of an airline ticket. Focusing on PNR treaties (Bellanova and Duez, 2012; Hobbing, 2010; for an analysis of PNR data, see Schreurs et al., 2008) and no-fly lists, he has pointed out that privacy practices in aviation are highly dependent on contextual factors that include the departing country as well as destination and itinerary and may even vary among different airports within one single country. A certain amount of those varying practices of collecting, processing and securing (and in the case of PNR: sharing) data is due to the highly fragmented nature of aviation. As Barros (2012) points out, national as well as EU legislation is complemented with binding

regulations (dependent on the membership of the respective country) from several international organizations (IATA, ICAO). Moreover, numerous countries have established distinct bilateral treaties for the purpose of establishing trusted traveler schemes and the sharing of passenger information as well. In addition to this fragmented legal situation, airports as the places of screening and control are often hybrid spaces that consist of a variety of public-private partnerships, outsourcing and subcontracting. Thus, empirically a large variance in collecting and handling of privacy-related passenger data already can be found today. The rise of risk in aviation consequently not only reinforces a general tendency in post-9/11 security thinking, but also the ongoing convergence of the public and the private sector. Concepts like the "Checkpoint of the Future" and "Better Security" indeed enact a long term trend, as has been suggested by Lyon (2006a), and draw critique not only in terms of privacy infringements. Attention should also be paid to the social sorting power of risk in mobility, possibly favoring wealthy elites who profit from facilitated travel, easier access to services and preferred treatment. The poorer and less mobile parts of the population, on the contrary, appear to be risky from the start, merely for not creating strong data trails in the international aviation system. And in risk governance, leaving no paper trail at all equals being a potential offender.

Conclusions: blurring the state and the market!

A number of normative problems remain with the use of risk as a governing tool, one of the most pressing issues being its relation to privacy. Risk assessment is based on personal information, rationalized in the calculation of profiles in order to sort mobile populations. In aviation security, it comes into being via the collection and processing of passenger data which represents the 'hard facts' on which the probabilistic rationale of risk governance must rely. Among the increasing number of security-related societal areas that are governed by risk, aviation is one of the most widely recognized, representing an environment that Lyon (2006a) has described as laboratory in which emerging technologies are deployed at early stages, only to be later spilled over into other, wider societal areas. Data collection at the airport is increasingly characterized by sharing between the private sector and public authorities. Commercial trusted traveler schemes have been identified a major asset in risk-based security governance, providing a valuable source for more 'hard facts', and thus contributing to more fine-grained risk assessment. Public authorities (Accenture, 2007; European Commission, 2011c) as well as private sector and industry initiatives (ACI/AEA, 2011; IATA, 2011; ICAO, 2012) have recently explored the possibilities of increased information sharing and risk assessment in order to address pressing needs in aviation.

Thinking about privacy, there is a double concern with this move. Not only do trusted traveler schemes require the disclosure of additional and sensitive personal data, but contextual limitations seem to put restraints on the individual capacity to circumvent data collection practices. Especially in "alienating and individualizing" (Augé, 2006) non-places like the airport, data collection is destined to be the way to enroll the passenger "into regimes of identification and authentication – through profiles, screens, anticipations and rules" (Adey et al., 2012: 173). Contemporary security governance enacts a shift away from discipline to risk (Amoore and de Goede, 2005: 150), aiming at statistical anticipation and precautionary measures rather than being incident driven (European Commission, 2012e: 12). At the airport though, pretty much both forms can be encountered. A priori risk assessment via data analysis cannot fully replace, but rather assist physical screening at the checkpoint. The individual thus

remains with the responsibility to ensure that both data profile as well as behavior are not deviant from the norm, unless one is willing to run the risk of being classified as a high-risk passenger and a potential offender. However, the general focus in risk regimes is shifting away from situational crime prevention that lays its scope on the immanent security breach in form of forbidden objects and materials, and towards an estimation of the likelihood of deviant individual behavior. Airports remain disciplinary spaces, but discipline is being altered. Turning the rationale of identifying high-risk passengers upside down, the exploitation of trusted traveler programs offers the possibility for passengers to enroll themselves not only into a scheme of futuristic technological gadgets, but also into a regime of self-governance, actively reducing their own risk score. Arguably, this might be the last bit of self-determined action for the individual, since aviation security as well as the spatial setup of the airport are strictly regulating behavior and movement. As Adey et al. (2012: 185) conclude, "this withdrawal of agency from the passenger reaches its apotheosis in contemporary aeromobility where the passenger has no choice but to yield to protocological control techniques that work to pacify the body such that it is light enough to be carried", being cleared of all doubts in terms of risk because his or her identity has been revealed through the gathering of intelligence.

The term 'trusted traveler', as it is commonly used, appears overly euphemistic, considering the fact that being trusted in aviation security actually means not being suspected to be an offender as much as everyone else. In exchange for this small but significant difference, a large amount of personal information has to be disclosed, depending on the nature and scope of the program. The large number of different trusted traveler schemes, the 'messy' and unclear international dimension of aviation security, including bilateral and multilateral treaties, as well as the changing actor constellation at airports make it difficult to answer the initial question of an impact of recent developments on privacy. However, this paper has argued that we find a number of different effects on the theoretical level. On the one hand, the scope on trusted traveler schemes as information assets in risk assessment reinforces the tension between the concept of privacy and security. Conceptualizing aviation security regimes as governance processes, it has been shown that commercial sector operations and law enforcement indeed converge in terms of data sharing, blurring the dimensions of privacy. On the other hand, the opt-in nature of trusted traveler schemes brings hidden data collection practices back to the realm of visibility and individual agency. However, it seems more than reasonable to question the voluntary nature of a self-determined submission of personal information when this enhances the chances of less invasive screening. In order to make a statement about concrete impacts of risk governance on privacy, empirical case studies appear destined to the tool of choice. Due to the fragmented nature of the topic, Privacy Impact Assessments (PIA) (Clarke, 2009) can help to put actual trusted traveler schemes into the applicable legal context and raise awareness for privacy issues in the aviation context, as well as stress available legal tools to ensure adequate data processing.

Risk-based security concepts like "Better Security" and the "Checkpoint of the Future" aim at bridging the (already minimal) gap between situational crime prevention and a full-range encoding of the individual into a system of surveillance, calculation and prediction. The aviation sector seems indeed "driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole" (Haggerty and Ericson, 2000: 610), with trusted traveler schemes appearing to be a key factor in this desire. Thus, passengers become partly persuaded and partly scared into the disclosure of personal information. Benefits like lounge access or fast lanes provide major incentives, while ever-more invasive primary screening measures kindle the desire to be exempted from at least

parts of the procedure. From a privacy perspective, risk-based security frameworks have raised increasing discomfort in terms of data collection, sharing, and processing between public authorities and the private sector. As Thatcher (2008: 266) has noted, “already, the boundaries between the public and private sectors are being eroded as far as access to personal communications data is concerned and an artificial distinction between the two is increasingly difficult to draw.”

[Inquiry 2]

Humor at the Airport? Visualization, Exposure, and Laughter in the "War on Terror"

With the emergence of aviation as a target for terrorism and serious crime in the 1970s, the affective dimension of airport security arguably changed dramatically. While flying had been framed as the fashionable, elegant and careless way of travel for the wealthy elites in its primal days (Curry, 2004), the proverbial lift-off into the "jet age" (Fuller and Harley, 2004) of aviation in the 1960s has opened up air travel for the masses – and along with the benefits of increased revenue came the risks that emerged from suddenly having to manage large mobile populations. Under the impression of hijackings and bombings, the security screening checkpoint was quickly transformed into a space of seriousness. Since the fatal consequences of airport security breaches had been witnessed by then, checkpoint operations subsequently started to enact a 'no bullshit' approach completely devoid of aviation's original 'lightness'. Thus, flying has gone a long way from its carefree early days to being a key element in the contemporary paradigm of critical infrastructure and national security that must not be tinkered with – and certainly not be joked about. Over the past decades, ever more security technologies have found their way into the checkpoints of airports worldwide on a regular basis, with body scanners being one of the latest innovations (Abeyratne, 2010; Frimpong, 2011; Nagenborg, 2011).

While having been established in airport security in the US and other countries for quite some time now, body scanner technology has arrived at the European Union relatively late. Body scanners were mentioned in the draft for Regulation (EC) No 300/2008 for the first time, but were eventually removed from the final version due to pending concerns in terms of health protection, privacy and data protection uttered by the European Parliament (Mordini, 2010; Barros, 2012). Although the technology was officially off the political agenda for the time being, several EU member states established trial runs to explore the suitability of body scanners for the everyday airport environment. Being among this group of 'test countries', the German Federal Ministry of the Interior (BMI) decided to deploy two machines during a trial run at Hamburg airport from 27 September 2010 to 31 July 2011. In the follow-up of the several trial runs in member states, the European Commission once again took the initiative and reported to the European Parliament and the Council in 2010 (European Commission, 2010a), building on the national experiences and calling for harmonized legislation at the EU level. This time, the European Parliament supported the initiative, however not without implementing "provisions on the protection of health, privacy, personal data and fundamental rights to technological progress" (European Parliament, 2011: 7). Thus, on 11 November 2011, Regulation (EU) No 1147/2011 eventually added body scanners to the list of allowed screening measures at European airports.

This paper looks into the social dimension and the interactive dynamics that emerge from body scanner technology in everyday use in an actual airport environment. In particular, we seek to address the encounter of humorous interaction between passengers and security personnel when faced with the notion of uncovering the fleshly body. We claim that a new mode of visualization through body scanners at the security checkpoint breaks open a rare space for humor in the 'war on terror', albeit a highly special and constrained one. We thus argue that aspects of exposure and shame become crucial in the crossing of the checkpoint, ultimately undermining the carefully engineered zones of different affective states at the airport (Adey, 2008a; Salter, 2007) and eventually creating a rift in an otherwise disciplinary

security regime. Within this rift, the use of spontaneously emerging jokes becomes enabled by the visual presence of the body. However, there is a sharp distinction between the venture of anxiety through a jest and the strategic upset of a security regime through humor. The 'bomb joke' remains a threat to the seriousness of the 'war on terror' and thus remains excluded from the space of humor.

This paper proceeds through the empirical encounters of laughter in an actual airport environment featuring body scanners. The ensuing section then sets the analytical stage with a brief conceptualization of distinct modes of humor, before the actual analysis sets the scope on the complex relationships between visualization, shame, exposure and the human body, as well as the emergence of particular modes of humor against the backdrop of affective engineering at the airport and the solemnity of the 'war on terror' in general. We argue here that unlike the strategic notion of carefully prepared and staged jokes, the type of humor encountered around the body scanners is a spontaneous and benign one that emerges from the bodily experience and seeks to handle an uncomfortable situation of visualization, shame and exposure.

Laughter in the forbidden zone: empirical encounters

In order to explore if and how social interaction would become affected by the use of body scanner technology, we conducted field research during the German trial run at Hamburg airport in June 2011. Being granted an access-all-areas status by the Federal Police, we tried to approach the screening checkpoint with a blank mind – but one thing that took us completely by surprise was the rather jolly atmosphere around the two body scanners that were in use at Hamburg airport. It took us by surprise even more so when compared against academic work on body scanners (Amoore and Hall, 2009; Magnet and Rodgers, 2012; Redden and Terry, 2013) as well as reports from actual airport practice (Harrington, 2014) that put emphasis on violations of bodily integrity and the potential for abuse of asymmetrical power relations between security personnel and passengers. As Harrington (2014) states for the US context, "just as the long-suffering American public waiting on those security lines suspected, jokes about the passengers ran rampant among my TSA colleagues." The crucial point here seems to be the mode of joking. While reportedly racist and sexist were made *about* passengers in the US, most of the humorous encounters at Hamburg airport went on *between* security officers and passengers.

In fact, every now and then, the interaction between the security personnel and passengers shifted into an openly humorous mode. This was not constantly the case, but nonetheless a noticeable distinction from the neighboring lanes equipped with metal detection portals. Drawing on personal experience as well as professional knowledge, humor was among the last phenomena we had expected to be confronted with. Indeed, as Kuipers (2011: 69) notes, humor is usually regulated by "humour regimes [that] are clearly bounded: they declare some topics off-limits and endow some with more rights to speak in jest than others." This regulation is presumably even stricter in spaces of discipline such as the airport, that has been deemed as a "total institution" (Salter, 2008c; Molotch, 2012) and that enrolls passengers into rigid security regimes via surveillance, biometrics and the digital encoding of the individual (Adey, 2004a; 2004b; Lyon, 2003a; Salter, 2008a). Even more so, as Bissell et al. (2012: 704) rightly add, the regulation of humor at the airport is achieved via "the spatial ordering of the aeromobile environment, which determines where laughter is appropriate." Adey (2008a) thus argues that distinct affective zones can be achieved through architectural planning. A

light and jolly mood is highly appreciated in the shopping mall parts of the airport, whereas in security operations, seriousness prevails and humor is explicitly banned – making a bomb joke in the face of a security officer can even lead to severe legal consequences (Martin, 2010). Thus, the question that emerged from our fieldwork encounters was: How was this 'return of laughter' to the screening checkpoint possible? Which contextual factors enabled the use of humor in a space which remains the last part of the airport where security is enacted on an interactive social basis, whereas the overwhelming part of the security framework relies on algorithmic risk calculations (Amoore, 2011; Amoore and de Goede, 2005; Lyon, 2006a; Salter, 2008b) and biometric identifiers (Adey, 2009; Lyon, 2008; Zureik and Hindle, 2004)?

Surprisingly, and contrary to the large account of literature on humor in general and in a multitude of everyday as well as special contexts, little explicit engagement with humor and security in the 'war on terror' has taken place so far. Some remarkable works that engage with the regulation of humor at the airport (Salter, 2011a; Bissell et al., 2012; Martin, 2010) do so from the perspective of a conflict approach to humor, thus setting the scope on how humor potentially can upset the regulations of the behavioral regime and expose and ridicule security screening. From this point of view, humor appears an improbable mode in the face of authority, as can be witnessed by the severe legal consequences of performing bomb jokes during screening. However, looking at studies that analyze humor in other seemingly improbable spaces like prisons (Nielsen, 2011), hospitals (Coser, 1959) or among sex workers (Sanders, 2004), the emergence of laughter in rather earnest contexts appears not to be improbable after all. But the 'war on terror' so far seems to be excluded from those funny notions and rather demands an unquestionable attitude of seriousness from everyone involved in it – from policy makers and practitioners to the individual who ultimately becomes the target and subject of security measures. And there appears to be little chance for laughter, as security regimes enroll the individual into behavioral protocols without room for deviance. The one who acts deviant by default draws attention and requires further scrutiny, risking serious consequences such as in-depth questioning, searches and even detention.

In an attempt to break with this rigid protocol of solemnity and to open up a space for laughter by uncovering apparent absurdities in the narrative of the 'war on terror', Heath-Kelly (2012) puts forward the question "Can we laugh yet?" And although she makes some excellent points about comical contradictions in extremism prevention programs and the use of drones, it appears that on the practical everyday level, the question must be answered with a 'no' – we can't laugh yet. We can make fun about security from a safe distance, but we cannot laugh in the face of the security officer. Obviously, comedians and cartoonist have engaged with the humorous potential of security technologies such as drones or body scanners. As Salter (2011a: 35) notes, "the shoe bomber, the No-Fly list, and the new millimeter wave scanner were each quickly made fun of through editorial cartoons, late-night comedians, on the Internet, and through commercials." And yet there is little potential for humorous resistance against security practices that would certainly appear funny in an absurd way if not for the solemn backdrop of the 'war on terror'.

At the airport, this paradigm of seriousness has in fact been on the rise since the 1970s, when in response to the occurrence of bombings and hijackings, the security checkpoint was turned into an area of earnest scrutiny without margin for error (Harrison, 2009; Sweet, 2009; Elias, 2010). Operating under the constant threat that carelessness could cause the next catastrophe, humor was explicitly banned from the checkpoint in particular. As indicated before, we had been taken by surprise when encountering the jolly atmosphere at the

checkpoint lanes equipped with body scanners, especially as opposed to the rather earnest and dull 'business as usual' at the neighboring lanes that featured regular metal detection portals. Humor has been identified as a transformative tool, able to render interaction into a "play frame" (Coates, 2007) that avoids, mitigates, or even resolves conflict. Given the need for more systematic research on the role of humor in the 'war on terror', this paper seeks to address a gap in terms of questions of the conditions under which humor can emerge. For the analyzed context of body scanners at the airport, we put forward a symbolic interactionist reading and claim that a rather benign form of humor emerged as a "coping strategy" (Sanders, 2004) that could momentarily break open both the power differential between traveler and security officer and the disciplinary frame of the airport itself. Furthermore, we argue that body scanners amplify the "panoptic gaze" (Foucault, 1977) that the individual is confronted with in an architecture that is driven by the overarching paradigm of maximum security. By uncovering the fleshly body and intruding the sphere of intimacy, body scanners appear to trigger the use of humor as an ice-breaker between strangers (Kuipers, 2008: 370) that unites passengers and security personnel in order to cope with anxiety and unease caused by the new visual element in screening operations.

What we laugh at: different forms of humor

In order to provide some conceptual clarity, this section explores the fragmented and "fuzzy-edged category" (Nielsen, 2011) that is humor. Academic readings of humor include functionalist, symbolic interactionist, phenomenological as well as conflict approaches (Kuipers, 2008). Following Mulkay's (1988) distinction of spontaneous and standardized humor, we advance here a contextual understanding that juxtaposes two distinct lenses: (1) the strategic, staged forms of telling 'canned' jokes that end with a prepared punchline and potentially attack the security regime of the airport; and (2) spontaneous, unplanned outbursts of benign laughter that emerge from situational context and that arguably can be traced back to the introduction of the visualization of the corporeal. As Fine and de Soucey (2005: 18) have noted, "it is not only that we joke in social settings, but that our joking is *from* social settings [emph. in. orig.]", thus the ideal typical juxtaposition arguably can contribute to an understanding of how spaces of laughter can break open even within the regulated affective zone of the checkpoint and to why specific modes of exposing the 'funny' characteristics of security (i.e., the 'bomb joke') remain banned.

> A passenger steps out of the body scanner and at the far end of the machine, he is being instructed to stop and take a look at the monitor that displays the results. The security officer, with a big gesture and a smile on his face, points to the monitor and exclaims: "And here's your photo!" The passenger seems confused for a second, but then his face lightens up and he responds: "I don't really recognize myself...oh wait, now I can see it!" Both share a laugh. (Field Journal, 8 June 2011).

This situation does not appear to be particularly funny to the uninvolved beholder. However, contrary to body scanners deployed at US airports, the devices at Hamburg airport[2] featured

[2] The deployed model was the "ProVision ATD" by L3 Communications, featuring a so-called "automatic target detection" software. See http://www.sds.l-3com.com/advancedimaging/provision-at.htm (accessed 31 March 2014).

a privacy-preserving software that did not display the original image of the scan – the one that is often being referred to as a 'naked' image – but an abstract matchstick figure on which, in case of a detection, the according body parts for manual secondary screening were indicated with a yellow coloring. Thus, the passenger and the security officer never looked at an actual picture. More importantly, the transfer of the individual image into a generic matchstick figure removes the result from the realm of identification. But nonetheless the officer addressed the matchstick figure as a photo and the passenger joined in on that willingly distorted perception of reality. And as it made them both laugh, there must have been something funny to it. In order to get a better notion of the social dynamics behind the emergence of laughter in this particular context, we put forward a reading of the bomb joke "as a weapon, a form of attack, a means of defense" (Kuipers, 2008: 372) that in conflict situations can "[poke] a hole through often-undiscussed but official versions of everyday reality, exposing their contradictions and the arbitrary basis of their social power" (Paolucci and Richardson, 2006: 334). Hence, the reluctance of airport security to allow such a mode of desecrating the earnest nature of the 'war on terror'. On the contrary, the seemingly harmless joking around the body scanners that we found empirically rather suggests a symbolic interactionist understanding of re-framing a situation that appears uncomfortable for everyone involved in it.

A sociology of humor has to cope with the fact that "disputes about the meaning of humour can never be settled" (Kuipers, 2011: 70). In order to conceptualize what is actually funny, one first has to come to terms with a terminology that features a plethora of fine-tuned concepts and labels such as joke, jest, funny, comic, mirth, jocularity, wit or satire (Palmer, 1994: 6), that carry different, but often overlapping notions. A lot of things can make us laugh – from plain tomfoolery to sophisticated observations – and the emergence of laughter depends on contextual factors as well as on the relationship between speaker and audience (Zijderveld, 1968). Moreover, as Kuipers (2008: 389) notes, "there is no necessary one-on-one relationship between humor and laughter", thus rendering laughter as the explicit aim of humor, but not as a causal effect. In order to work, humor needs to rely on a certain common ground and a shared definition of a situation (Nielsen, 2011) that eventually unfold the funny elements that make us laugh. A conflict approach reading of humor builds on an explicit aim that requires careful preparation and a notion of formalization. This particular mode of humor can be encountered in numerous forms – as written texts, comics, cartoons, images, in songs and movies, or as jokes and anecdotes. What they all have in common is the setting of a stage, the creation of a shared ground in which the punch-line will ultimately reveal the funny element and release the carefully constructed suspension. The punchline itself in this case unravels "humor as a radical activity that attacks social structure by delegitimizing its most sacred aspects (especially its traditional norms and institutions)" (Davis, 1995: 335). The careful setting up of a stage thus enables the speaker to make fun of elites, denounce social injustice, or utter complaints about particular issues or society in general (Zijderveld, 1968). What we find here is an "unmasking function of joking [that] consists mostly of the fact that a socially accepted or traditional meaning structure is exposed to a totally different meaning structure" (Zijderveld, 1968: 304), while the author/speaker hides behind the protecting wall of laughter without being held responsible for the obvious "gap between what is said and what is meant" (Coates, 2007: 32). This double move of speaking the truth/making fun has indeed been a powerful one throughout history. As Amoore and Hall (2013: 99) note in examining institutionalized forms of speaking the truth/making fun and their proximity to sovereign power, "the themes of subversion and mockery are found throughout the long and knotted cultural history of the fool, the clown and the trickster." However, the use of humor works in

both directions of the social spectrum. Not only can making fun from the bottom of the social ladder expose the powerful elites, but humor can also operate from a position of strength – momentarily blurring the hierarchical space, for instance between managers and the workforce, or between a company and its customers.

Bissell et al. (2012) have addressed one of the few humorous breaks in aviation security with their analysis of the 2009 Air New Zealand campaign, featuring an in-flight safety instructions video that "shows airline staff wearing nothing but G-strings, shoes, and body paint" (Bissell et al., 2012: 696). Referred to as the "Bare Essentials" safety video and being part of a campaign entitled "Nothing to Hide", the strategic goal here becomes quite clear: apart from drawing the viewer's attention, the reference to nudity demonstrates to the customers a maximum of transparency while at the same time the introduction of fun into the otherwise serious matter of emergency preparation establishes a friendly relationship between the company and the travelers – while still emphasizing the message that Air New Zealand cares very much about the safety of their customers. However, when measured against the backdrop of the carefully engineered zones of affective states to be encountered at the airport, it becomes clear that light and happy moods are actually something that is very much desired at all stages of air travel – with the crucial exception of the security checkpoint.

The space of screening is set to momentarily strip the atmosphere of all that might interfere with the operation to unravel the truth about the traveler and their intentions. As Salter (2007: 59) argues, "the power of the state to expel or exclude any traveler, even citizens with no cause or appeal, is internalized into an anxiety of the confession" and thus enacts an "emotional state of the passenger – affected by the airport environment – [that] is meant to literally close-off the passenger's capacity to disrupt the security processing system through, for example, walking the wrong way, or by telling a joke or misbehaving" (Adey, 2008a: 445). While being heavily regulated within security operations, the restrictions on humor do not at all apply to other parts of the aviation experience, enabling Air New Zealand to bond with their customers through humorous videos and in general enabling airport operators to create an affective state of relaxation and passenger convenience, contributing to the purpose of the shopping malls that contemporary airports have been turned into.

On the other side of the conceptual spectrum, the symbolic interactionist reading we put forward here "focuses on the role of humor in the construction of meanings and social relations in social interaction" (Kuipers, 2008: 377). Laughter can indeed emerge from intuitive interactions that cannot build on the time-consuming telling of a joke or an anecdote, but that rather happen in an unplanned fashion. In this case, the spontaneous reaction to the contextual environment, as opposed to the careful setting of a stage, suggests a common construction of an interpretive frame (Goffman, 1974). It is the non-reproducible situation that is instantly rendered funny by a remark, a look, a gesture, or even a lifted eyebrow and that only makes sense for the involved individuals in the specific situational context. A symbolic interactionist approach thus enables a reading of humor "at the heart of social analysis, crucial to the shaping of meanings, situations, selves, and relationships" (Kuipers, 2008: 379-380). What we find here instead is the emergence of laughter that does not carry the notion of social critique or other strategic elements, but a form of humor that rather unites the participants of the particular situation, establishing a notion of community and shared burden, even when this practice does not change the situation after all.

> A passenger, after stepping out of the body scanner and looking at the monitor that displays the abstract matchstick figure for a second, proclaims: "That's me? It doesn't show my belly!" He, the security officer and several surrounding people (both travelers and security officers) burst out in laughter. (Field Journal, 9 June 2011)

> Another passenger, before entering the body scanner, asks the security officer in an altered voice: "Is there anything I can do to look good?" Several people laugh at that remark, including the security officer. (Field Journal, 9 June 2011)

> A passenger makes an over-exaggeratedly sad face when looking at the results of his scan, then laughingly exclaims: "Can't I see my picture? That's a shame!" (Field Journal, 9 June 2011)

Those and similar situations occurred in quite a high frequency during our observations at the two security lanes equipped with body scanners, independent of gender, nationality, or ethnicity. A hint for a meaningful interpretation of those types of situations comes from Coser (1959), who has described laughter in reference to anxiety about oneself. She emphasizes that in order "to participate in jocular talk one has to have overcome one's worst fears and be somewhat detached" (Coser, 1959: 179) from what is actually at stake. The issue at stake here – apart from the anxiety to be singled out and to be denied to continue the airbound journey – appears to be the bodily integrity and the expectation of becoming the target of a machine gaze. The misleading media coverage on body scanners supposedly had a major impact here. After all, German news media had published scan pictures of US machines without privacy-preserving software and had been referring to the devices as 'naked scanners'. Thus, it can be assumed that there was increased unease about the production of an accurate image of what lies hidden underneath the clothing, thus revealing the arguably most intimate parts of the human body and deeply intruding into the individuals' intimacy. Uncertainty and anxiety about the aesthetics of the corporeal body prevail as the unveiling of the secrets of the flesh becomes inevitable. The spontaneous emergence of humorous comments in this context, so we argue, frames a shameful complaint against what is going on – a complaint that must not be uttered in a direct form, as open confrontation at the security checkpoint is not something a traveler would be advised to perform. As Bergson (1911) has noted more than a hundred years ago, the humorist appears as a moralist in disguise – expressing unease about security practices that intrude the individual's most intimate sphere, although not in a confronting fashion, but in this case rather shifting to the presumably safer ground of simply laughing about oneself.

The efforts to spontaneously turn a serious encounter into a jest thus can be interpreted as a coping strategy to protect oneself from contextual pressures (Sanders, 2004). As Tiessen (2011: 177) argues, "the mere presence of the scanners during the security check endows them with legitimacy as they participate in actively reshaping the whole security environment – the anxieties of the travelers, the apparent expertise and power of the security staff, the apparent efficacy of the security measures." Once the dreaded situation is over, humor also appears as a form of relief. When passengers looked at the results of their scan, expecting the worst – seeing themselves naked, with all the deviance their own body would reveal from whatever ideal of beauty it would be measured by – but eventually rather seeing a matchstick figure with a smiley face, they were able to release the pressure by ironically referring to

themselves as 'the one with the belly' or 'the one who thinks it was a shame that no actual photo appeared on the screen'.

The multiple dimensions, modes and functions of humor in the realms of the social and the societal are certainly much more diverse than described in this section, but the construction of two ideal types arguably facilitates the analysis of our empirical encounters at Hamburg airport. The juxtaposition of strategic and spontaneous forms of humor adds an understanding to our initial surprise about the laughter around the body scanners and contributes to a reading of momentarily breaking up carefully engineered affective zones of air travel. However, laughter at the body scanner does not mean that security would not be taken seriously anymore. On the contrary, what we experienced was that the security personnel had an impressive sensitivity for the boundaries of humor. When the atmosphere was about to turn into open tomfoolery, they quickly stopped the joking (though, in some cases with a fine sense of humor themselves, as one security officer referred to the body scanner as "not a joke box" ["keine Witzbox"], Field Journal, 9 June 2011). After all, there is an almost 'natural' power imbalance between passengers and security officers at the airport, as the latter ultimately choose how social interaction can be (re-)framed. This puts considerable emphasis on questions of agency and institutional constraints. When, as Harrington (2014) reports, at US airports images from body scanners reinforced "all the old, crass stereotypes about race and genitalia size [that] thrived on our secure government radio channels", this falls in fact well in line with the argument that "women, minorities, and the poor tend to be subjected to greater transportation burdens than their male, White, and relatively affluent counterparts" (Monahan, 2009: 298). How can we then explain the rather benign practices of joking we encountered at Hamburg airport, where fun was not primarily made *of* passengers, but where humor resulted from social interaction across the power gap?

Mitigating conflict?

As the socially constructed meaning of humor is deeply embedded in situational context, airport security depicts a distinct constellation that challenges humor by contrasting it with the seemingly absolute claim of security and its connected earnest atmosphere. The ensuing question then is: how are both modes balanced (Salter, 2011a: 35)? In explicitly addressing humor in conflict situations, Norrick and Spitz (2008: 1668-9) have identified four ways of concluding conflict sequences: (1) submission, (2) compromise, (3) stand-off or (4) withdrawal, with the two latter not solving the conflict situation, but rather postponing it (Norrick and Spitz, 2008: 1669). This leaves submission and compromise on the table. However, keeping in mind the inherent power differential between the traveler and the security regime of the airport, the unease about revealing the fleshly body to the artificial gaze of the scanner is not a conflict situation that offers leverage for bilateral negotiations. The traveler afraid of the body scanner might offer concessions, but protocol leaves no room for bargaining with the security officer. As Molotch (2012: 96) notes, a compromise disqualifies for security operations, as "standard security operating procedure assumes single and unvarying focus for all, a meta-message of authority not to be trifled with." Security screening is part of the game of air travel, including the option of refusal – only that in this case, there would not be any air travel after all. The checkpoint requires absolute submission. Molotch (2012: 91) subsequently argues that "moving through security resembles a prison routine not only in the submissiveness required but also in the standardization of the equipment as well as the sharp limits on what can be done with it." Thus, if "body scanners compel passengers to *perform*

submissiveness [emph. in. orig.]" (Tiessen, 2011: 177), laughter does not influence the outcome of the conflict situation, but rather serves as a "safety valve" (Coser, 1959) that mitigates the defeat that is submission to the scan. Such a humorous re-framing of situations that would otherwise not be interpreted as particularly funny arguably could lead to laughter at something that in other contexts would be dismissed as stupid or offensive. But while appearing as a "superficial and helpless gesture in the face of power" (de Goede, 2005: 389) from a conflict approach angle, a reading of laughter as a spontaneous attempt to relieve individual anxiety and nervousness (Kuipers, 2008: 389) seems to be a more appropriate interpretation.

As Norrick and Spitz (2008: 1670) note, the attempt to introduce humorous elements into the conflict talk by one side can lead to either acceptance, a reciprocal shift to the level of humor or to rejection. By intuition, one would expect the latter from a conflict situation at the airport checkpoint. Not only from the notion that jokes about bombs have been banned from security operations, but also from the professional distance that security officers keep from their 'customers'. As one security officer told us during an interview, security staff tries not to engage emotionally with passengers and thus rather opts to "treat them like objects [own translation]" (Interview, 17 January 2013). Molotch (2012: 96) adds here that "for security personnel, accepting a display of good humor risks accepting passenger moves that are outside the serious business of proceeding in the prescribed order from point A to point B." Part of the engineering of the solemn affective state of the security checkpoint is also the power differential between the traveler and the security officer. Though formally being the paying customer, the passenger has no option but to enact submission to the rules of the checkpoint, and the security officers are well aware of the fact that they are not to be fooled around with. Otherwise, they have measures to make sure that "if somebody likes to joke around, I can show them who is boss [own translation]" (Interview, 17 January 2013). However, what we encountered at Hamburg airport was not only acceptance and mutual jests – as often as not humor was in fact introduced by the security officers themselves.

> After a negative result of the scanning procedure, a passenger looks puzzled at the green "OK" symbol on the screen. When being asked: "What did you expect?", he uncertainly responds: "I don't know...maybe scissors in my stomach." The security officer, with a pretended seriousness, replies: "Why, did you swallow scissors?" Then both burst out in laughter. (Field Journal, 8 June 2011)

> An obviously very nervous and anxious passenger steps into the scanner. Before initiating the scan, the security officer proclaims: "And now smile!" The passenger smiles. Similar events occur with a high frequency. (Field Journal, 9 June 2011)

By default, a good security officer at the airport screening checkpoint must be a sensitive person with a talent to deal with the various different emotional states of passengers that approach the checkpoint. Traveling can be a lot of stress – for those who are not used to doing it regularly, but also for those who operate on tight schedules. Such sensitivity, obviously, is not always a given and the lack thereof can possibly result in degrading and discriminating practices, especially as the gaze of the machine targets the human body (Magnet and Rodgers, 2012; Redden and Terry, 2013; Harrington, 2014). As Amoore and Hall (2009: 451) note, "it is the intertwining of security practices with new understandings of the body – no longer

machine, or territory, but digitised information to be 'read' – that critical challenges must grapple with." In today's airport environments that are indeed fully digitized with their online check-ins and automatic access controls, the screening checkpoint remains the sole space of mandatory social interaction – and at the same time the most likely space of conflict due to liquid bans, forbidden objects and delays. The use of humor thus appears a reasonable tool to mitigate the inevitable, but still remains highly unlikely when measured against the stakes of the 'war on terror'. Given the specific nature of the funny interventions at the body scanner introduced by security officers, it becomes clear that the target of the humor here is indeed the flesh and the anxiety thereof. To request a passenger to smile during the scan while being perfectly aware that the result will not be a photographic image but a matchstick figure visualization – that will appropriately enough smile anyway – turns out to be a typical move. The activity of watching can be unpleasant not only for the watched but for the watcher as well. Or, more precisely: for the person who operates the machine gaze of the body scanner. Thus, we suggest that the use of body scanners opens up a space for humor from both sides of the power continuum. And while the passenger's anxiety appears to be a reasonable explanation for the mitigating effects of spontaneous outbursts of laughter, the use of humor on the side of the security personnel seems to show a more general unease with the visualizing notion of the body scanner. We thus argue that what we can find here is an increased production of shame and exposure that leads to the momentary crumbling of the otherwise carefully engineered affective zones at the airport. After all, "the human body – its legal and moral status, its value, its meanings, and the way in which technologies modify it – lies at the heart of the body scanner debate" (HIDE and RISE Projects, 2010: 25).

Zooming in closer on the body

The encountered humorous breaks overwhelmingly were uttered as expressions of anxiety towards the body, rendering the fleshly confession and the submission to the machine gaze of the scanner as the focal point of both fear and relief that were eventually re-framed into a jocular interpretation. Body scanners have been connected with the violation of bodily integrity, inevitably crossing the commonly established line between the outer appearance and the highly intimate zone of the body. As Hildebrandt et al. (undated: 18) state, "one of the purposes of clothes is to cover parts of the human body that are considered extremely personal and exposure of which is only acceptable in intimate personal contexts." The context of an airport screening checkpoint, however, is anything but personal. The very purpose of security regimes is to break up the individual, extract whatever information can be extracted and separate them from the sphere of subjectivity. The ensuing "data doubles" (Haggerty and Ericson, 2000) turn out to be partly machine readable, enabling algorithmic risk calculations and 'smart' monitoring of possibly deviant behavior, and partly remain within the dichotomous logic of suspicion/non-suspicion, which can only be cleared by zooming in on the physical and stripping the mobile body of all objects that are considered dangerous. However, what is left of the visuality of the body when it appears only momentarily in the code and then instantly re-disappears in the software that is set up to preserve the traveler's privacy? It has been argued – in particular for the German trial run – that involuntarily exposing the hidden corporeal is nothing to worry about once the visualization of the flesh has been covered with a friendly-looking, anonymous matchstick figure (BMI, 2011). Thus, there is no actual 'nudity' to be found thanks to the privacy-preserving software features, but yet the notion of exposure remains connected to the scanning procedure. Juxtaposing the unveiled physical nudity that

becomes re-veiled through digital code with a psychological notion of nakedness arguably provides a better understanding for the production of shame and unease.

> Imposed "virtual" nakedness is an important threat to bodily and psychological integrity. Nakedness is more than nudity. While nudity is the simple state of absence of clothing, nakedness is a mental state, which implies being stripped of decency, to lack an element of protection. Nakedness involves objectification, the process of symbolically turning a person into an object to be appraised [emph. in orig.] (HIDE and RISE Projects, 2010: 32).

Read through that lens, the unease with body scanners stems not so much from the actual production of a 'picture', but rather from the inevitable zooming in on the body. A procedure in which a machine enacts a gaze at the fleshly, corporeal intimacy that would never be exposed in contexts different than the most intimate, leaves the travelers in a puzzled state of mind, wondering "does it cross the lines of decency and their expectations for privacy?" (Tiessen, 2011: 168). In this double twist of targeting but not showing, of gazing but re-concealing, we argue, lies a key element to understanding the unprecedented emergence of humor. Bellanova and González Fuster (2013) have tagged this simultaneous unveiling/re-veiling of the flesh as "bodies-scanner setting", as opposed to the original notion of the scanner that genuinely visualizes the body, and hinting at an arrangement that deliberately removes the 'naked' image from the checkpoint but leaves the scanning procedure as such openly and intimidatory on the table. In the crossing of the checkpoint, the body itself clearly remains the center of the screening operation, being a key element of authorization for proceeding to the next stage of air travel by revealing its harmlessness. Yet, in a move of seeing/not seeing, the specter of the flesh overshadows the scenery of the security checkpoint, as "*disappeared elements* haunt the stabilization of the setting and remain thus somehow *present* [emph. in orig.]" (Bellanova and González Fuster, 2013: 204). Introducing a matchstick figure in order to conceal the original image of the 'naked' body has been a crafty move to resolve a number of legal issues in terms of privacy, and maybe it even possesses the potential to disrupt the "logics of disembodied control at a distance" (Monahan, 2009: 287) that are so inherent to modern surveillance measures, and that enabled security officers in the US to (secretly) make fun of passengers over their secured radio channel. Indeed, as Harrington writes, "many of the images we gawked at were of overweight people, their every fold and dimple on full awful display." Such depiction of the human body had been erased from the machines at Hamburg airport – but arguably, a smiling abstraction has nevertheless not resolved the unease of the machine gaze; the anxiety of the virtual strip; the unspoken evaluation of what is hidden beneath the clothing; and the scope on the corporeal, fleshly body, that otherwise would only be revealed in situations of utmost intimacy.

> A passenger steps out of the scanner and looks puzzled at the green "OK" symbol on the screen: "I can't see anything!" The security officer replies: "That's because everything was OK." The passenger laughs nervously and says: "Oh, and I thought one could see the whole body." (Field Journal, 8 June 2011)

As Amoore and Hall (2009: 451) have noted, "the body does not remain 'untainted' by being exposed, even if the data collection leaves its surface intact." Similarly, the argument here is that body scanners impose a bodily experience of scrutiny and mental 'nakedness' that has a

major impact on the traveler, even if there is no 'real nudity'. The machine gaze appears to unfold a transformative power that affects how airport screening procedures are being perceived. Arguably, in the 'haunted' production of shame and exposure through unveiling/re-veiling processes of visualization, we can find the urge to break the habit of the earnest. The reasons for that, so we would suspect, are to be found in the lacking ability to express the increasing amount of unease in direct confrontation. Thus, a symbolic interactionist reading of our empirical encounters puts forward a conceptualization of the realm of the funny that creates an exceptional break from standard protocol in the 'war on terror', and transforms the experience of nakedness into what appears as a collective complaint that remains unspoken, but nonetheless comes to the surface in spontaneous outbursts of anxiety and relief. As Coser (1959: 180) argues, "humor allows the participants, in a brief span of time and with a minimum of effort, mutually to reinterpret their experiences, to entertain, reassure, and communicate." In the context of security screening, this mutual reinsurance appears to enable passengers to effectively cope with the gaze of the body scanner. After all, apparently we can find limited spaces for humor in the 'war on terror', and if only for the struggle with visualization, exposure and shame.

Conclusions – exposure, shame, and the failure of affective engineering

Before summing up the connection between visualization, exposure, shame, laughter, and the momentary crumbling of affective engineering, the empirical foundations of this paper should be given some consideration. Our data only provides insight into a very specific national context for a limited period of time. It thus might be argued that our analysis represents a situation that created a special exceptional state of social interaction – within the more general reading of the 'war on terror' as its own state of exception (Agamben, 2005). Thus, it appears difficult to generalize our findings, especially when compared to reports about body scanner practices in the US that included a malicious use of humor towards "the bodies of Othered subjects who fail to pass the checkpoint, or who are disproportionately adversely affected or violated in the screening process" (Magnet and Rodgers, 2012: 107). After all, the trial run at Hamburg airport temporarily transformed the screening checkpoint into a spectacular arena built around a new and presumably daring experience of the flesh. The environment in which we found ourselves might thus be mistaken for a glamorous break in the otherwise dull and never-changing routine enactment of screening protocol. However, the empirical encounter turned out to be a different one. Our field research fell into the final days of the 10-months duration of the trial run, when media attention had long shifted to other topics. Thus, the overall activity at the checkpoint rather appeared as 'business as usual'. Yet still, except for the frequently flying business people, the situation of facing a body scanner turned out be a first-time experience for most passengers. And the security personnel operating the checkpoint lanes told us that they were not really used to working with the body scanners as well.

As a consequence, it might be argued that the occurrence of humor and laughter could simply stem from the fact that the inhabitants of the checkpoint were faced with a new and challenging situation. Body scanners had not been deployed in Germany before, and unease towards an unfamiliar technology and an unknown screening procedure might have been the cause for nervous laughter. Moreover, the use of the body scanners was based on the voluntary nature of the travelers. Only two of the 12 lanes were equipped with the machines, and passengers were pointed to the voluntary basis of the trial run with signs and video

screens in the area in front of the security checkpoint. This could have prevented overly anxious or suspicious persons from stepping into the body scanner in the first place. We had to deal with those empirical constraints, but still faced the unique opportunity to conduct field work during the only regular deployment of body scanners at a German airport security checkpoint up to date.[3]

As has been shown throughout this paper, the relation between humor and contemporary security regimes is a difficult one. Airports as particular spaces of the 'war on terror' have been turned not only into "difference machines" (Adey, 2008b), but also into places of affective engineering – allowing light and jolly moods in the commercial areas while enacting a strict and solemn protocol at the checkpoint. When it comes to the merciless mechanisms of screening, "bringing the fleshy, anatomical body into view gestures not only to the capacity of the visual to provide ultimate authentication but also to a fidelity to the truth of interiority, where the penetrative gaze can reveal that which is concealed" (Bissell et al., 2012: 697). Software solutions attempt to re-conceal the body once the image of the flesh has been produced, but, so we argue, the machine gaze itself produces a haunting imagery of mental nakedness, so that the corporeal dominates the checkpoint regardless of privacy-preserving tools and produces a deep anxiety that eventually vents in humorous breaks. Our symbolic interactionist interpretation of those breaks as a re-framing offers a reading that is distinct from previous attempts that conceptualized the use of humor as a conflict tool that challenges security practices. However, the rather benign form of humor encountered in our fieldwork turned out to be acceptable for as long as it did not desecrate the "confessionary complex" (Salter, 2007) of the airport. After all, one must on no account let the terrorist slip through the tight grid of security measures simply because one was joking around and not paying the adequate attention. Thus, taking up Heath-Kelly's question once again: maybe we actually can laugh, but only in a certain and limited way.

Or, putting the question differently: is there a politics of laughter involved in the crossing of the checkpoint? In fact, such a deliberate politics of laughter by default appears unlikely, given the lack of social cohesion and the institutional constraints of the airport security regime. However, the jocular re-framing of potential conflict situations allowed both passengers and security personnel to master the potentially violent scanning procedure in a dignified fashion. Thus, arguably, the admissibility of humor strongly depends on how the laughter emerges. It is fine to share a jest when confronted with frightening technology such as body scanners, making the process of visualization an unpleasant one for both the watched and the watcher, and it is also fine to reassure the startled passenger with a funny remark and signal that everything is alright. This in fact hints at a certain degree of 'political' agency that security officers were allowed to apply at Hamburg airport. But behold if humor is used as a strategic weapon to unmask the apparent absurdities in the 'war on terror'. Telling a bomb joke is a powerful tool to unveil the "security theater" (Schneier, 2006) that is being performed at sites of security operations. As Martin (2010: 27) analyzes, "a bomb joke *declares* the concrete possibility of violence, but *implies* the passenger's innocence [emph. in orig.]", thus intentionally creating a false positive that unsettles the calm environment of security nonetheless. It is the move of telling one thing/meaning another that creates an upheaval in

[3] Since the end of 2012, all major German airports offering connections to the USA have started installing body scanners, but not within the framework of the regular screening checkpoint, but merely for use as a secondary screening measure for US-bound flights, as required by the US Department of Homeland Security (DHS).

the truth-finding complex of security and that has led to the fact that “at security, one must be cautious with humor” (Molotch, 2012: 94).

To be sure, the asymmetrical power relations between security officers and passengers were at no point in question, and “the promise to build ‘anonymity’ into technologies […] in order to ‘protect privacy’ does not address the violence involved in uncovering, breaking down and writing the body into digital form” (Amoore and Hall, 2009: 451). However, the spontaneous use of humor by both passengers and security officers, so we argue, can be conceptualized as intuitive behavior that emerged from visualization, shame, and exposure. As a response to the targeting of the corporeal, humor has enabled the involved individuals to re-interpret the situation and create a jocular atmosphere that was able to briefly bypass the seriousness of security operations. After all, even the strictest behavioral protocol and affective engineering cannot fully prevent outliers. As Adey (2008a: 448) notes, “not everyone has to follow the route intended for them by the airport authorities, not everyone will be enticed to buy and more relevantly, nor is everyone limited in their capacity to act or feel.” Despite remaining reluctant to put forward a politics of laughter, we thus conclude that such a humorous mode appears not as inappropriate as could be expected from the literature on humor in security contexts. As has become apparent throughout this paper, the notion of the body is indeed a powerful one, endorsed by anxiety towards nudity/nakedness and the revelation of what by default should remain in the realm of the private and intimate. Thus, instead of a politics of laughter, it appears more appropriate to speak of an intuition of laughter – one that nonetheless performed exceptionally well in the face of the artificial gaze of the scanner. After all, “what turns nudity into nakedness is degradation” (HIDE and RISE Projects, 2010: 33), and such degradation depends heavily on the social practices and their particular contexts. In our fieldwork, the (veiled) notion of the flesh appeared indeed so strong that it eventually enabled spontaneous outbursts of humor and laughter, momentarily breaking open a space for benign humor in the otherwise solemn and earnest ‘war on terror’. Admittedly, it is a small space, and it calls for more empirical research in the distinct security regimes that incorporate body scanners, but it is a notable one nevertheless.

[Inquiry 3]

Privacy and security – on the evolution of a European conflict

Privacy and security have often been framed as conflicting concepts that must be conceived of as incommensurable and thus constitute a trade-off (van Lieshout et al., 2013). And although such a notion has been largely criticized for using under-complex definitions of both privacy and security, as well as for neglecting empirical examples of positive sum games and questions of whose privacy and whose security are affected (Valkenburg, 2014), the trade-off model appears quite persistent. Considering the contemporary nature of data-driven security measures, much digital ink has been spilled about the presumably weak standing of privacy in the face of a more or less overwhelming context of (inter-)national security (see for instance Bennett, 2005; Leese, 2013; Nissenbaum, 2010; Tsoukala, 2010). This paper analyzes how the relation between privacy and security has been framed and re-framed in the field of European security research, eventually ending up as a question of privacy by design. Privacy by design, so the argument goes, enables new security technologies to be both privacy-preserving as well as effective and efficient, and thus would ultimately serve as the silver bullet that resolves the conflict/trade-off. However, this paper puts forward the claim that the notion of privacy by design rather puts old wine into new bottles, as a closer look reveals that the core problem is not tackled, but only re-framed according to the general technical scope of security research. Thus, it appears that the new emphasis on privacy and the ensuing argumentative mitigation of the conflict merely intends to comply with the EU's increased focus on normative security and at the same time renders research governance as a technological fix for the technological fix that security is conceptualized as in the first place.

The paper proceeds by providing a brief overview of the emergence of security research at the EU level over the last decade and sheds light on its underlying rationalities, *en passant* retracing how the presumed trade-off between privacy and security was framed and eventually evolved into a privacy by design approach alongside the emergence of a more normatively coined EU 'security project'. The paper concludes with a critical assessment that questions the suitability of privacy by design as the panacea that it comes advertised as.

EU security research – on the emergence of a field and a conflict

"Security research is the new guy in town" (Burgess, 2011: 2). As opposed to 'traditional' fields of research funded by the European Union, research that is explicitly dedicated to the security of the EU and its citizens has only been around for the relatively short term of about a decade (Burgess, 2011; Bigo and Jeandesboz, 2010; ECORYS, 2009), and has at times struggled to find its niche among related fields with a strong 'security touch', such as for instance Information and Communication Technologies (ICTs). However, fostered by 'new' and global threat scenarios, the quest for appropriate remedies has become an integral part of the realm of fundamental and applied research that is set to produce new tools and technologies, and thus to contribute to effectively establishing security in the European Union – or so the argument goes. Arguably, the need for reinforced security solutions has been catalyzed by the debate that was kindled by the events of 9/11 and their massive aftermath in terms of security policy

adjustments.[4] In the EU, security is now conceived of as a cross-cutting concept that has to tackle widespread areas such as terrorism, serious and organised crime, cybercrime, cross-border crime, violence itself, and natural and man-made disasters (European Union, 2010: 14-16). Thus, security research has eventually been established as a key area within the European funding framework.

This very framework, however, is currently undergoing structural change. In 2014, EU research funding has hit an institutional threshold as the established Framework Programmes (FP) come to an end with FP7 and will be replaced by an overhauled, streamlined, and arguably simplified and more efficient program entitled Horizon 2020.[5] Official documents promise that this new framework will, amongst other, set clearer scopes on societal issues, most notably privacy and data protection (European Commission, 2011d). Thus, this structural change appears an appropriate break to analyze how the still emerging field of security research is being (re-)shaped alongside economic rationalities and the emergence of a European 'security project' itself, and how the relationship between privacy and security keeps evolving. In order to set out an analytical framework, this paper argues that EU security research funding follows two main trajectories: it is mainly conceived of as (1) a means to foster the European economy, and (2) as a primarily technical framework that aims to produce specific solutions to clearly defined security problems. In recent years, however, a third notion has been added to this dichotomy, as 'security' itself is now increasingly presented as a normatively embedded concept that needs to comply with human rights and civil liberties. This appears to be a major reason for abandoning the trade-off model and the search for new and integrative approaches, eventually ending up with privacy by design.

'Historically' speaking, EU security research can be framed as a field that has been shaped through an inextricable entanglement with the industrial sector, as has been compellingly shown by Bigo, Jeandesboz, Hayes, and others (Bigo and Jeandesboz, 2010; Hayes, 2006; 2009). Multiple companies and personalities from the branch have been involved in setting up of the field and the intensified cooperation between the Commission and the industry, taking off in 2003 with the establishment of the *Group of Personalities in the Field of Security Research* (GoP, 2004) and the initiation of the *Preparatory Action on Security Research* (PASR) in 2004. The GoP was eventually followed up by the *European Security: High Level Study on Threats, Responses and Relevant Technologies* (ESSTRT) in 2006 and the setting up of the *European Security Research Advisory Board* (ESRAB, 2006) in 2005 and the *European Security Research Innovation Forum* (ESRIF, 2009) in 2008, both of which further envisioned the future of security research at the EU level.

Throughout the published reports of the aforementioned fora, particularly privacy and data protection have been framed as disruptive elements for security technologies and thus for the overall goal of a secure European Union. For instance, as Bigo and Jeandesboz (2010: 6) have pointed out, the ESSTRT final report frames the conflict such that "the underlying assumption is that intrusiveness is a requirement for efficiency, and that privacy undermines efficiency", and the ESRAB report states that "research into ethics and privacy, and the trade-off between improved security and loss of privacy, will influence technology development and in parallel address aspects of how citizens perceptive security and insecurity" (European Security

[4] It should be noted, however, that the notion of a post-9/11 'break' in terms of security policy has been contested such that recent developments should rather be seen as part of a larger historical trajectory (Lyon, 2003a).

[5] For an overview of Horizon 2020, see http://ec.europa.eu/programmes/horizon2020/ (accessed 7 July 2014).

Research Advisory Board, 2006: 8). Thus, privacy and security were generally conceived of as incommensurable concepts, and it was very clear where the preferences for effective security research had to be placed – the need for security apparently trumped the need for privacy. Either security measures would work, and this would be because they would be based on a sufficiently large database that allowed for glimpses of the future and the next event that needs to be canceled out – or they wouldn't work because privacy claims and the restrictions of the data protection framework would thwart their effectiveness. More or less independent of any actual conceptualizations of privacy, be it as the classical "right to be left alone" (Warren and Brandeis, 1890) that entails a "boundary control process" (Altman, 1977: 67), as the "claim of an individual to determine what information about himself of herself should be known to others" (Westin, 2003: 431) which in terms involves "a constraint on the use of power" (Regan, 2011: 498), or politically as the foundation of the democratic constitutional state (Friedewald et al., 2010: 62) - any position that values the (digital) personal sphere would be considered disruptive from an industry point of view. Especially when taking into consideration Helen Nissenbaum's (2010) concept of privacy in context, one might indeed be inclined to say that threat scenarios were used to create a contextual override for privacy arguments.

As mentioned earlier, such a trade-off model is certainly oversimplified, and arguably only represents a part of the full story. How come we find such a striking neglect of privacy arguments in official documents, then? The next section aims at unpacking the underlying notions of security and security research in the European Union. It will become clear that EU security research unfolds along a clear-cut economic agenda, and thus introduces a very specific and market-driven approach to the relationship between privacy and security.

Economics and technologies

First trajectory. Both FP7 and Horizon 2020 documents acknowledge the economic goals identified by the Europe 2020 strategy (European Commission, 2010b), framing "research and innovation as central to achieving the objectives of smart, sustainable and inclusive growth" (European Commission, 2011b: 2). The underlying rationale, as stated by the Staff Working Paper on Horizon 2020, is that "modern economic theory unanimously recognises that research and innovation are prerequisites for the creation of more and better jobs, for productivity growth and competitiveness, and for structural economic growth" (European Commission, 2011d: 7). For that purpose, a study on behalf of DG Industry & Enterprise has analyzed the global security market and the position of the European security industry, coming to the conclusion that "it appears vital to stimulate and create a proper innovation framework in the security domain and establish fast track development procedures for new market technology requirements" (ECORYS, 2009: xvii). As a consequence from those findings, the European Commission in 2012 adopted an "Action Plan for an innovative and competitive Security Industry" (European Commission, 2012a) in order to secure and extend market shares in a rapidly growing global security economy.

In the same year, the Commission published a document on EU security research entitled "Safeguarding Society, Boosting Growth" (European Commission, 2012c). Overlooking its content, it quickly becomes clear that the emphasis lies on the latter part, as the document states that

> our objective, notably through our Security Industrial Policy initiative, is to improve the global competitiveness of the EU security industry by stimulating its growth, invest in the research and development of future, world-leading security technologies and processes, and launch any effort necessary to overcome the current market fragmentation for security products in the EU and thus establish a true Internal Market (European Commission, 2012c: 1).

In fact, the conceptualization of EU research funding as a policy tool for economic growth has always been out in the open. Particularly, the purpose of security research can be identified by its institutional location. The housing within DG Enterprise and Industry instead of the maybe more natural fit DG Research & Innovation indeed provides a clear statement and has been criticized for its "significant consequences for the way we understand and do research on security as an ethically charged field of research" (Burgess, 2011: 1). This general economic scope will likely be reinforced with the start of Horizon 2020. As the joint communication on the new framework states, "since the launch of the Seventh Framework Programme (FP7), the economic context has changed dramatically" (European Commission, 2011a: 2), and now urges the EU to provide even stronger incentives, since "research and innovation help deliver jobs, prosperity, quality of life and global public goods" (European Commission, 2011a: 2).

The ECORYS report on the competitiveness of the European security industry bolsters those general assumptions with factual numbers. The global security market is estimated to be worth €100 billion, with the size of the European market in the range of €26 to €36.5 billion (ECORYS, 2009: v). This translates into roughly 180,000 employees in the European security sector. Accordingly, security research receives a considerable amount of funding, with the security theme under the FP7 being worth an overall amount of €1.4 billion (European Commission, 2012c: 2) and the financial terms for the "Secure Societies" action under Horizon 2020 alone determined at €1.7 billion. However, despite those efforts, the ECORYS report points out a "low aggregate level of EU funding for security-related research, technology development and innovation (ECORYS, 2009: x). In a comparative perspective, EU security research funding still remains "considerably below the efforts made in the USA", leading to "potential weaknesses in the underlying competitiveness of the EU security sector" (ECORYS, 2009: 38). This could in terms lead to a predicted loss of market shares to a low of 20% in 2020 (European Commission, 2012a: 2), particularly with the Asian security industry massively catching up in the high-tech area, but also with considerable competition from Russia and Israel (ECORYS, 2009: 51-60). The remedy for such a threatening scenario appears quite simple: reinforcement of market stimulation through enhanced security research funding and faster product cycles (ECORYS, 2009: xvii). Thus, one might indeed be inclined to agree with Bill Clinton's famous statement that "it's the economy, stupid." Economic prosperity has been the driving force behind European integration from the beginning, and why should it change within security research, of all things?

The Action Plan for the security industry subsequently provides concrete steps of action in order to reinforce the competitiveness of the European security industry, suggesting the creation of a true Internal Market through favorable conditions, the enhancement of competition and lower production costs, as well as strengthened support for SMEs (European Commission, 2012a: 3). Apart from those issues, however, one of the most pressing concerns still appears to be the potential of privacy and data protection to thwart the effectiveness of security technologies and thus their successful market impact in the first place. Subsequently, the Action Plan takes up on that conflict and states that a major problem arising from the

societal dimension of security research is the social acceptance of security technologies – or rather the lack thereof, which could result in a number of negative consequences for the security industry, i.e. wasted investments (European Commission, 2012a: 5). Most strikingly, privacy requirements are regarded to hurt the security market on both supply and demand side. For the supply side (i.e. the European security industry), this would mean that its products might not reach their maximum 'security potential' due to constraints in data collection and analysis, and "for the demand side it means being forced to purchase a less controversial product which however does not entirely fulfill the security requirements" (European Commission, 2012a: 5). Thus, from an industry angle, the situation appears quite clear: privacy hampers security. Or rather, it hampers security technologies, as EU security research is indeed primarily locked in on the emergence of new technologies.

Second trajectory. The rationale behind this scope becomes clearer when looking at how current security efforts within the EU are conceptualized as data-driven and risk-mitigating measures. As security policies increasingly emphasize the potential of databases, data-sharing and interoperability for the purpose of gathering knowledge and thus being able to prevent future risks (see for instance Amoore, 2009; Geyer, 2008; Leese, 2013; Marx and Muschert, 2007; de Hert and Bellanova, 2011), Information and Communication Technologies (ICTs) have spilled over into security contexts – and with them issues of privacy (and data protection). Security technologies heavily focus on communication, social networks, and other forms of individual interaction with a digitized everyday environment, such as sensors or biometrics. The massive amount of personal and behavioral data constantly produced then serves as the basis for fighting crime and terrorism through various forms of data exploitation such as algorithmic profiling and probabilistic risk calculations (see for instance van Otterlo, 2013; McCue, 2007; de Pauw et al., 2011). Or, put more simply: security itself has indeed become dominated by the desire to accumulate data in order to predict the future and counter-act criminal and terrorist incidents. But when security is supposed to be enacted through mitigation of future risks, those risks first have to be identified.

ICTs have emerged as the very tools to do so, and such a notion has obviously evoked critical reactions. Thus, ICT research ethics have specifically been concerned with the implications of the use of personal information in distinct contexts (Wright, 2011). Arguably, the increasing spill-over of ICTs into the realm of security is also the reason why privacy and data protection are framed as predominant ethical concerns of current security research within official EU documents. Whether or not this limitation of ethical concerns to one clear-cut area is by any means adequate remains questionable. It should clearly be noted that multiple other pending ethical issues such as autonomy, social inclusion, human dignity, or dual use and function creep/mission creep between the civil and the military realm of security also do require attention.

However, when looking at the political and financial efforts put into security research over the last decade, one might indeed be under the impression that "our political masters, aided and abetted by the security industry, often appear willing to sacrifice some of the citizenry's privacy in order to better secure society", as van Lieshout et al. (2013: 120) have provocatively formulated it. Thus, how come the stark contrast of a presumed trade-off was eventually transformed and is now conceived of as a resolvable privacy by design issue instead of the irreconcilable conflict that it was before?

A normative turn?

The answer arguably lies in the re-framing of the overall European 'security project'. With the Treaty of Lisbon in 2009 and the ensuing legally binding status of the European Charter of Fundamental Rights (European Union, 2000), the EU has – at least on paper – made a clear commitment to human rights and civil liberties. For the (broader) field of security, this commitment is reflected in the European Internal Security Strategy (European Union, 2010) of 2010 and the Stockholm Programme that provides the current concrete policy framework (2010-14) (European Council, 2010). The Internal Security Strategy, for instance, explicitly states that "Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity" (European Union, 2010: 8). And the Stockholm Programme puts forward a Europe built on human rights, and goes as far as to claim that when it comes to security measures,

> "basic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established" (European Council, 2010: 10).

This strengthened emphasis on normative aspects of security can also be found in the FP7 security scheme, claiming that "the potential impact of the resulting technologies and activities on Fundamental Rights, ethical principles and societal values should be addressed as part of the proposed research" (European Commission, 2012d: 10). Again, especially privacy and data protection have thus been officially tagged as norms that potentially become infringed by security technologies (European Commission, 2012b). Apart from such official statements, the predominantly technological security tools that have emerged from the FP frameworks in recent years have become the target of normative interventions due to their potential negative impact on society (Geyer, 2008; Guild and Carrera, 2010).

Third trajectory. Alongside this new scope on the normative dimension of security, research funding, or rather the governance thereof, is also undergoing change. Security research now has to be 'ethically compliant' in order to take into account possible negative impacts on the societal level. Security research projects are thus to be accompanied by the explicit coverage of ethics boards in order to ensure that research is in line with normative principles. Subsequently, research ethics have come to enact a key role in the governance of security research, and are set to establish safeguards against detrimental societal impacts of security technologies at an early stage during research and development. In EU research funding, a dedicated ethical coverage of the research process has been introduced as "fundamental ethical principles" (Stengel and Nagenborg, undated: 2) since FP5 (1998-2002). Particularly, fields such as medical and biological research have a long history of a need for ethical coverage, as has become apparent by the emerging possibilities of 'engineering' human life at the genetic or molecular level. Security research is joining those fields as one of the areas that has be monitored and advised closely. As Burgess (2011: 2) notes, "security comes with its own special ethical baggage", since it carries the potential to inflict curtailments on fundamental societal and individual values. In fact, numerous scholars have in recent years engaged with the threatening and negative consequences of new and emerging security

technologies (see for instance Salter, 2008e; Bigo and Tsoukala, 2008a; Monahan, 2006b; Lyon, 2006b; Amoore and de Goede, 2008b).

However, on the other hand, security itself represents an important value as it "embodies the social and cultural needs of a society, its hopes and fears, its past and its ambitions for the future" (Burgess, 2011: 2). Read through that lens, security represents its own ethics as an overarching prerequisite for any society. Much has been written on the problems that can arise from over-emphasized security and ensuing detrimental impacts on human rights and civil liberties (for a comprehensive account, see Waldron, 2003). Adding to that list of potential negative consequences, security research

> can include particular measures that have as a secondary effect an increase in insecurity – such as the development of scanning devices that cause unease, weapons systems that provoke fear or insecurity among innocent bystanders, or surveillance systems that are experienced as too invasive (Burgess, 2012).

Thus, security research appears a Janus-faced phenomenon that possesses the potential of both detrimental and beneficial outcomes that indeed come as "inseparably intertwined" (Burgess, 2012). The delicate balance of the 'goods' and 'bads' of security for society subsequently underlies constant challenges through security research and the technological tools that emerge from it. A close look reveals, as mentioned earlier, that nearly all security-related research projects within FP7 do feature a technological scope, as "the Security theme supports R&D actions oriented towards new methodologies and technologies."[6] Due to the sketched potential detrimental impact of security technologies on societies, coupled with the financial volume of security research funding, the stakes for particular security research ethics appear exceptionally high (Burgess, 2011). This constellation is indeed reflected in official documents – and once again it is predominantly framed in terms of privacy. The last call fiche for the security theme of FP7, for instance, states that "if ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity" (European Commission, 2012d), and the EC document on ethical and regulatory issues in research policy dedicates a whole chapter to "New Security Technologies and Privacy" (European Commission, 2012b: ch. 2).

This emphasis on privacy arguably comes from the aforementioned data-driven nature of contemporary security technologies that build on the collection and analysis of large amounts of data, as well as from the well-defined legal applicability of the data protection framework that gives privacy concerns a 'procedural advantage' over other normative concerns when it comes to security technologies. The interesting fact is now, that with this 'new' scope on morally right security, the original conflict between security and privacy becomes rather reinforced than mitigated. In other words: with the increased emphasis on the importance of privacy, the privacy side of the original equation has been upgraded and is now not so likely to be overridden by security anymore. And since there no longer seems to be an *a priori* choice which part of the equation should be more cherished, the decisive question then becomes: how to possibly resolve this dilemma and reconcile privacy and security such that their relationship complies with the upgraded normative take on security within the EU? The answer appears indeed an intriguing one: if it is not possible to overcome the conflicting

[6] http://cordis.europa.eu/fp7/security/about-security_en.html (accessed 7 July 2014).

positions of the trade-off (however oversimplified they appear), why not abandon the model, after all? The ensuing move beyond, as enthusiastically announced, has eventually resulted in privacy by design.

Privacy by design: a technological fix for a technological fix?

In the effort to effectively govern emerging technologies from security research, the Commission has identified three main dimensions of regulatory privacy protection: (1) technical, (2) legal, and (3) self-regulatory (European Commission, 2012b: 20). Characteristically for the legal dimension is its rather spatial scope, as it is based on the European Convention on Human Rights (European Court of Human Rights/Council of Europe, 2010) and the European Charter of Fundamental Rights (European Union, 2000), rendering its power strongly connected to the jurisdiction of the EU. Within this jurisdiction, legal privacy and data protection provisions possess an enforceable status and thus provides strong incentives for any supplier of security technologies to stay within the explicitly formulated boundaries of data collection and processing. However, in times of global data flows, such a (supra-)national regulation appears hardly up to the task of effective privacy protection.

The self-regulatory dimension of security research governance, on the contrary, is based on voluntary commitments from the private sector. Self-regulation towards technology development that fulfills ethical requirements then is set to be achieved through the involvement of stakeholders and the establishment of 'soft' regulations (European Commission, 2012b: 20). The scope within self-regulatory governance lies on non-enforceable concepts such as "market self-regulation, corporate social responsibility (CSR), and governmental incentives for research that can drive technology towards more ethical development" (European Commission, 2012b: 20). Albeit admitting the potential of voluntary forms of research governance, Székely et al. (2011: 183) have pointed out that monitoring and supervision of self-regulation within the area of emerging technologies appears a highly difficult task.

Thus, the official position of the European Commission with regard to security research governance can be summarized such that "weaknesses in self-regulation and legal governance suggest technological governance as a good site for concrete, operationalized engagement with tensions between the protection of privacy and the pursuit of security" (European Commission, 2012b: 24). One might be inclined to say that this preference in fact appears a technological fix to right the technological fix that is security research in the first place. Now how to achieve such technological reconciliation? From the official documents, it becomes quite clear that Ann Cavoukian's concept of privacy by design see for instance (Cavoukian, 2009a; Cavoukian et al., 2010) is now considered to be the silver bullet for the old clash between security and privacy. Thus, researchers and developers are encouraged to tackle possible privacy and data protection issues pro-actively from the very beginning in order to avoid costly adjustments later on.

In fact, the ESRIF final report in 2009 made an early effort to bridge the gap between privacy and security and stated that "ESRIF advocates implementation of a 'privacy by design' data protection approach that should be part of an information system's architecture from the start" (European Security Research & Innovation Forum, 2009: 31). How does this work? Privacy by design starts with the assumption that "privacy is good for business" (Cavoukian et al., 2010: 405), and develops the idea that privacy can be conceived of as a positive sum game. This is a crucial notion, as it stands opposed to the postulated zero sum game that is central

to the hitherto dominant trade-off model. Furthermore, privacy safeguards then should be implemented proactively and early within the development and design of information processing technologies, and be built in a way that they last throughout the entire product life cycle.

Central in such a conceptualization of the relationship between technology and privacy/data protection is the assumption that privacy principles should be incorporated early in research and development in order to avoid costly retrofits at later stages (Cavoukian, 2009a). It is exactly this presupposition that is now mirrored in EU security research. As stated by the Commission, privacy by design "should be recognized as a guiding and technologically neutral principle, suitable for flexible applications, in a general provision mandating that existing privacy and data protection principles be integrated into ICTs" (European Commission, 2012b: 26). Just as well, the Action Plan for the security industry suggests to make use of a privacy by design approach (European Commission, 2012a: 11). This falls also well in line with recent discussions about privacy-preserving data mining and privacy-enhancing technologies (Custer et al., 2013; Aggarwal and Yu, 2008).

But does it really resolve the original conflict, namely the presumable choice between improved security or the protection of privacy? There are a number of issues to be found in the relationship of 'security and/vs privacy' that might not be elegantly resolved through privacy by design. A key element in privacy by design are the Fair Information Principles (FIPs), that are set "to limit collection, use and disclosure of personal data, to involve individuals in the data lifecycle, and to apply appropriate safeguards in a continuous manner" (Cavoukian et al., 2010: 406). Thus, as Schaar (2010: 267-8) argues, this means "the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible." Such practices are undeniably suitable for organizational and economic contexts. However, as has been argued throughout this paper, data-driven security technologies derive their added value exactly from the information surplus that is accumulated through collection and processing of data that could eventually be connected to possible criminals or terrorists in order to cancel out future risks. And we should remember that by the logic of security experts and policy makers, the more information one can get, the better the prediction of the future and thus the better our overall security will be. In other words: security cannot thrive on informational parsimony. FIPs on the contrary radically take away the possibilities that come with advanced analytics in security contexts. This stark contrast stunningly reminds of the early days of security research, when the "trade-off between improved security and loss of privacy" (European Security Research Advisory Board, 2006: 8) was openly framed as a major obstacle for the field. But how to achieve both effective security and non-intrusive privacy, then?

Certainly, there has been considerable progress in the techniques for data analytics. For instance, algorithms that allow for privacy-preserving ways of data mining (Aggarwal and Yu, 2008) have been on the rise in recent years. But even with such privacy-friendly methods of data collection/analytics, the tension between privacy and security cannot be fully resolved. The "dimensionality curse" (Aggarwal, 2007; Aggarwal and Yu, 2005) states that in order to fully preserve privacy, the amount of personal attributes would need to be reduced to such an extent that the utility of processing the data is lost. Hence, the contradicting interests between privacy on the one hand and the benefit of being able to process data on the other hand cannot simply be resolved using technical means. Thus, a certain conflict remains between efficiency in terms of the generation of security knowledge and the preservation of

privacy. In simple terms, the more (individual) attributes are reduced from the dataset, the less utility will emerge from analytics. Is the turn to privacy by design merely old wine in new bottles, then? Even if it does not convincingly resolve the tension between privacy and security, the transformative framing of the old 'conflict' tells us a lot about the current state of affairs with regard to privacy and security.

Conclusions

This paper has shown that the relationship between the concepts of privacy and security has come a long way from an early conceptualization as a sharp trade-off towards a contemporary framing as a technological issue that appears resolvable through privacy by design. However, this paper has put forward the claim that the current re-framing is not particularly well suited to actually mitigate or resolve the tension between privacy and security, but rather pays tribute to the technological scope on security, while at the same time acknowledging the increasingly normative take on security with the EU.

The trade-off model has always been troubled by the oversimplified claim that it was possible to put forward to unspecified concepts and outweigh them against each other. And while privacy has long been conceived of as "a moving target" (Friedewald et al., 2010: 61), the conceptualization of security is shifting as well. To stay within the metaphor, the second target is also starting to move quite rapidly, as the notion of security is undergoing deep-seated normative transformation. When thinking about the current relationship of privacy and security, it appears only appropriate to take into consideration the changing state of security between abstract concepts, concrete technological applications, economic desires and normative prerequisites and implications.

Is security merely a driver for economic growth and prosperity, or does it indeed come as an intrinsic value that has to be handled with care in order to avoid detrimental effects on societal values? Is privacy a value that is still trumped by the seemingly overarching desire for security, or does it have the capacity to challenge the paradigm of security through the EU's confession to more human rights and civil liberties based security measures and the further incorporation of ethics into EU funded research? The ensuing constellation appears a puzzling one: depending on the perspective, security (technology) is regarded as either a serious threat for privacy or an opportunity for massive economic revenue – but should security by default not be a value itself? A basic need for any society to ensure its present and future prosperity and a safeguard for its individuals to flourish and realize their potential?

It remains up for discussion whether privacy by design can provide a true reconciliation of privacy and security, or whether it solely serves as a veil that is set to obscure major concerns with regard to data-driven security technologies. It appears that such a technological approach to the governance of security research (and subsequently to 'security' itself) falls well in line with the general technological scope of EU security research. It remains open whether this 'technological fix for a technological fix' will strengthen the position of privacy and data protection, or whether security will further trump normative considerations and civil liberties/rights. To end on a critical note: privacy-by-design might not be the silver bullet that it is regarded to be right now, but might rather be a concept that at first sight appears to be easily applicable within the general technological paradigm of security, but only seemingly soothes the conflict between privacy and security.

[Inquiry 4]

Body scanners in Germany: a case of failed securitization

With Regulation (EU) 1147/2011 of 11 November 2011, the European Union has established the legal framework for the regular deployment of so-called 'Security Scanners' at EU airports. As a number of incidents of unlawful interference with aviation had revealed the limits of traditional security screening technologies in detecting criminal and/or terrorist attempts, a push had been made by stakeholders from aviation as well as policy makers towards a technology that arguably is more capable to detect hidden dangerous objects on passengers (Mordini, 2010). The machines – better known to the public as 'Body Scanners' or 'Naked Scanners'[7] – have since then been put to use in several member states, most notably in the UK and the Netherlands. Other countries like Germany, France and Italy have tested devices in trial run set-ups, but have not (yet) implemented the European regulation into national law, since they have deemed body scanners as not suitable for everyday use in an airport environment. This paper analyzes the German context, where body scanners have been tested in a trial run at Hamburg Airport from 27 September 2010 to 31 July 2011, after which the Federal Ministry of the Interior (BMI) decided not to implement the devices, claiming that they had not met the requirements of airport security authorities. This paper puts forward the claim that this failure of implementation relates to privacy claims that eventually disrupted the technological prerequisites of body scanners.

Body scanners as securitization

In order to understand the particular outcome of the German case, it is helpful to conceptualize the process of establishing a new security technology as a long-term securitization move, going back to research and development and the funding thereof. Scrutinizing how the securitization process failed in Germany, this paper thus contributes to an understudied area within securitization theory, as the major part of research analyzes successful securitization processes (Salter, 2011b). As to measure whether a securitization process can be deemed successful, Williams (2011) suggests a concept of intensification that moves beyond the dichotomy of normal politics vs exceptional politics, enabling the researcher to analyze more fine-grained securitization processes that remain below the level of extremity. According to this argument, existing issues that already have been securitized within the airport environment cover a wide range of dimensions that include materials (metal detection; the ban of liquids), objects (X-ray scans of suitcases and hand luggage; lists of forbidden objects), data (trusted/registered traveller programs; Passenger-Name-Record information, Advance Passenger Information), biometrics (iris scans; hand vein recognition) and space itself (smart CCTV surveillance; armed security guards). Arguably, the implementation of body scanners at the checkpoint intensifies security by expanding the

[7] The EU uses the term 'security scanner' as a "generic term used for a technology that is capable of detecting metallic and non-metallic objects hidden in clothing; whereas detection performance lies in the scanner's ability to detect any prohibited object that the person screened may be carrying concealed in their clothing" (European Parliament, 2011: 4). In order to avoid terminological confusion, this paper shall proceed to use the term 'body scanner', as it more accurately describes the functional logic of the technology – to depict the human body free from clothing in order to search dangerous and forbidden objects.

object dimension or even adding another dimension of securitization to this already impressive list, located on the axis between objects and biometrics. Although not being approached as an identifier, with the implementation of body scanner technology the human body itself becomes a target of careful scrutiny in order to reveal its possible hidden dangers.

Another suggestion to measure the success of securitization moves comes from Salter (2011b), who claims that the answer should be looked for in policy change and/or new, upgraded or converging executive competences. Following this argument, what can be found empirically is that at the European level, body scanner technology has been successfully implemented in the legal framework that provides the basis for aviation security which then has to be enacted by the member states. But while at the supranational level, the process has been completed, policy outcomes on the national level are varying. In the German context, no policy change in aviation security has occurred and authorities have not been willing to use body scanners on a regular basis. Thus, this paper claims that we are facing a failed case of securitization on the national level and seeks to understand the specific reasons for this failure.

From a Copenhagen School perspective (Buzan et al., 1998), the story of the failure to implement yet another layer of invasive screening technology at German airports is in fact a quick one to tell. As the empirical coverage of the trial run had shown, the machines had simply produced a too high number of false positives (passengers who had been wrongly identified as a threat), leading to an increased level of manual secondary screening, and thus turned out to be too slow for a security framework that is driven by an overarching paradigm of speed (Adey, 2006). While these results were in fact somewhat sobering for the authorities that originally had been in favour of the technology, they nonetheless quickly backed up the trial run. In a press statement released after the end of the test, the German Federal Minister of the Interior, Hans-Peter Friedrich, said: “The Federal Police will continue to closely accompany developments in this area, so that we will hopefully soon have machines available that meet our security demands as well as can process the number of passengers [own translation]” (BMI, 2011). Thus, the official position was to emphasize the dedication to stick to body scanner technology as a future remedy for aviation’s cross-pressures in terms of security, speed, cost-efficiency and customer convenience. While in the run-up to the trial run, doubts about privacy, images of the ‘naked’ human body and data protection as well as health issues had been uttered by representatives of the civil society, the authorities and the security industry reacted quickly and tackled those issues (Barros, 2012). The machines deployed in the German trial run most notably featured a privacy-by-design approach, replacing the images of ‘naked’ bodies with matchstick figures. Critique in terms of data protection had also been dealt with, as the possibility to store images had been removed. As Friedrich had framed it in a previous press statement: “Individual rights are to be maintained – this requirement is fully met. […] All data will be erased immediately after screening [own translation]” (BMI, 2010). Moreover, health issues were not confirmed by several studies on radiation, since devices in the EU were not using X-ray technology like comparable machines in the US, but terahertz technology. As a consequence, the main narrative of evaluation of the trial run in the public discourse was predominantly framed in numeric terms. Considering the overall costs, capacity, and false positives rate of the deployed machines, no reasonable cost efficiency could be established, subsequently leading to the non-implementation of the new screening layer.

Arguably though, a turn towards sociological approaches to securitization theory can contribute to a more detailed understanding of the specific conditions that have led to the failure of the implementation of a new security technology in one member state, while the securitization process has been successful in others. Bigo and other authors of the Paris School (Bigo, 2001; Bigo, 2008a; Bigo and Tsoukala, 2008b; Bigo and Walker, 2007) have identified a gap that needs to be addressed and filled in order to analyze how security comes into being in complex contemporary assemblages. Turning away from a scope on how security is being enacted through discursive states of insecurity and the creation of political realms of exception, they suggest a shift towards agencies and professionals of security, and their role in shaping security through bureaucratic processes and expert knowledge, thus involving a broader range of actors that usually do not appear at the level of public discourse. In this effort to connect IR theory and "the problem of the international" (Bigo and Walker, 2007) with political sociology, such an approach to securitization is rather interested in the untangling of practices and the contribution of professional knowledge. From this point of view, the Copenhagen perspective reflects only a certain amount of what happens in securitization processes, while the Paris framework proceeds beyond the surface of language. A scope on the practical dimension can provide value-added by "explicitly 'uncovering' dimensions of security formation that are commonly left implicit" (Huysmans, 2002: 52), or as Salter (2011b: 117) puts it: "a solely linguistic model cannot account for the politics of the securitization process."

Hence, this paper is based on a series of expert interviews (N=25) with representatives of stakeholders from the aviation security sector (airport operators, airlines, German Federal Police, private security companies), as well as experts from research and development and the security industry, who were able to provide in-depth detail knowledge on the trial run and the complex assemblage of actors and agencies in German aviation security. This paper argues that a long-term securitization move can be retraced to early stages of research and development, but that the ensuing securitization process was eventually disrupted by the privacy-by-design approach that was set to handle the doubts in terms of intimacy and images of the 'naked' body. While those doubts had effectively been tackled on the political and legal level with the use of matchstick figures in place of the original body images, this privacy-preserving solution induced a massive technological challenge on the level of research and development as well as industrial design which could not effectively be resolved. The machines with built-in privacy safeguards merely marked identified areas of the human body on the matchstick figure, indicating a need for manual secondary screening to the screening officer (Mordini, 2010). However, this procedure requires a highly reliable and accurate automatic threat detection in image analysis in order not to produce any false negatives (passengers with dangerous objects that are not identified as such). Since this requirement could not be met by the available machines, in an effort to prevent security breaches in a real airport environment during the trial run, the specifications for the level of threat detection had to be reconfigured and produced an exceptionally high number of false positives, leading to considerable delay in the screening process. As a consequence from those experiences, body scanners were eventually rejected by the German authorities – not as a direct consequence from privacy requirements, but as a consequence from the technological challenges imposed by the adjustment on the political level. Privacy-by-design had been leading to a causal chain of improper automatic threat object detection, an increased rate of false positives, and a considerably slowed down screening procedure. Linked to scarce

resources within the airport environment in terms of space and economic pressures, the conditions for a regular deployment of body scanners had effectively vanished.

The fragmented field of aviation

In sociological approaches to securitization research, several authors have taken up Foucault's thoughts on security governance and have pointed out the importance of a profound understanding of power relations among sector-specific actors that struggle over the shaping of apparatuses of security (Huysmans, 2002; Balzacq, 2010; Bigo, 2001; Bigo, 2002; Bigo, 2008a). Considering the Foucauldian (1980: 194) notion of the "dispositif", researchers are facing "a thoroughly heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions – in short, the said as much as the unsaid." A central argument brought forward by supporters of a sociological reading of securitization is that speech act analysis is only able to capture a certain amount of securitization processes (Bigo, 2001). And more importantly, that this part of the discourse is merely the one that is enacted by agents that possess enough power and resources to articulate themselves in what could be called the 'official' or 'visible' discourse. This is not to say that speech does not matter – on the contrary, the Copenhagen School has greatly contributed to the evolution of security studies. However in order to achieve a more profound understanding of how securitization comes into being at the 'grass-root' level, the Paris School can complement the analysis with a scope on security professionals and their expert knowledge in their particular field. As Salter (2007: 50) notes, this approach is particularly well-suited for aviation security, and more specifically for the screening checkpoint as the spatial arrangement where aviation security is enacted. Accordingly, this paper seeks to go beyond the speech act and shifts the scope of analysis to the operational level of aviation security. As Foucault (1980: 195) adds, a crucial element in this complex assemblage is the "formation which has as its major function at a given historical moment that of responding to an urgent need. The apparatus thus has a dominant strategic function [emph. in orig.]." Being a murky and fragmented field that features a multitude of stakeholder constellations and jurisdictions, a sociological approach to securitization is primed to analyze this strategic function within overlapping power structures and obscure networks that constitute securitization processes in aviation (Salter, 2007). In order to analyze security as a "dispositif emanating mainly, but not only, from a specific field of professionals" (Balzacq et al., 2010), Bigo et al. (2007) suggest to start with a topology of the field to be scrutinized.

Such an approach has particularly been applied in the works of Salter (2007; 2008c) in order to clarify diffuse powers and authorities at the airport as a specific form of governmentality. Regarding the two major cross-pressures (i.e. secure and efficient movement vs cost-benefit ratio) embedded in a general paradigm of risk assessment and risk management, security (and its potential breach) at the airport is being treated like a regular business asset (Salter, 2008c: 20). Dealing with securitization processes, stakeholder agendas and power relations are converging into the question of "how is it that international mobility and civil aviation came to be a problem that needed this array of solutions?" (Salter, 2008c: 22). Neglecting an overall teleological agenda of securitization in fragmented and dispersed aviation environments, Salter (2008c: 23) thus draws on the metaphor of the "rhizome" (Deleuze, 1992) that denies centralized control over a network of networks and rather constructs a framework that consists of autonomous, yet connected agents and agendas.

In this complex assemblage, the screening checkpoint in aviation security enacts Foucault's analysis of contemporary governance as a matter of "allowing circulations to take place, of controlling them, sifting the good and the bad" (Foucault, 2007: 65). Technology has been at the core of airport checkpoint set-ups for the purpose of scrutinizing the individual ever since aviation has been threatened by criminal and terrorist attempts. Airport security regulates and directs populations that are on the move, or more figuratively, 'flow' through the spatial arrangement of the airport. The valve of the screening checkpoint is set to sort out dangerous individuals from the passenger flow in order to prevent potential security breaches (Adey, 2004a; Adey, 2006; Jones, 2009) since the 1970s, when the first hijackings had emphasized the vulnerability of the aviation system and called for responsive action, eventually leading to metal detection and luggage screening (Sweet, 2009: ch. 2). In post-9/11 security regimes aviation has quickly been framed as critical infrastructure (Aradau, 2010) and thus has been a target for a number of securitization moves in the 'war on terror'. Airports in particular have been at the centre of public attention in recent years, as numerous (successful as well as thwarted) terrorist and criminal incidents have catalyzed the claim to upgrade screening with more capable technologies. As airports enact a key role in the international system, representing virtual borders (Lyon, 2003a: 13) as well as "symbols of mobility" (Adey, 2004a: 500), new security policies and the implementation of new and emerging technologies have indeed changed the landscape of aviation security in the aftermath of 9/11. As Szyliowicz (2004) somewhat drastically puts it, aviation security today very much equals homeland security, which on the other hand has become a problem of the international, as internal security and its external dimension increasingly converge (Eriksson and Rhinard, 2009).

Highlighting an often neglected area of security studies (Guittet and Jeandesboz, 2010), technology is a major factor in the checkpoint-centred security apparatuses of contemporary aviation. Enabling authorities to scrutinize, identify and sift the passenger flow, the technology-driven security approach at the airport provides both sophisticated surveillance systems and at the same time fosters the security industry, thus turning the attention to the role of high tech companies in the shaping of security (Lyon, 2006a: 406-7). In terms, this technocratic framework leads to a practice of increasingly implementing emerging technologies that have not been sufficiently tested. Accordingly, Bonß and Wagner (2012: 47) argue that some technologies have not been deployed at the airport yet simply because improperly designed machines would disrupt standard procedures in screening, leading to additional expenditures in terms of time and money. However, as Buzan and Hansen (2009: 54-7) note, key events have always played a role in shaping the evolution of security (studies). Airport security can indeed by reconstructed as an incident-driven chain of policy moves (Lyon, 2003a: 16). More recent policy changes in the 'war on terror' have featured responses to such terrorist attempts as the 2001 shoe bomber, the 2006 liquids plot or the 2009 underpants bomber (Jacobson, 2012: 36). Thus, as part of an emerging European security agenda, aviation became a key part of post-9/11 EU level efforts.

Prior to 9/11, the European Union had not played a role in aviation security which was until then enacted via intergovernmental standards of the International Civil Aviation Organization (ICAO) and its European subgroup ECAC (European Civil Aviation Conference), as well as the International Air Transportation Association (IATA). Only in the aftermath of 9/11, the European Union became actively involved in legally structuring the field and tackling security issues (Barros, 2012). Regulation (EC) 2320/2002 established a common ground for binding regulations in EU aviation security. In 2008, when Regulation (EC) 300/2008 was set to replenish the former legislation, body scanner technology was included in the draft regulation

for the first time as an additional permitted screening measure at airports. However, with pending questions on health protection, privacy and data protection, the European Parliament blocked the draft regulation and called for a comprehensive ethical and legal impact assessment (Mordini, 2010: 173), eventually leading to the omission of body scanner technology in the final version of the regulation. The issue then remained on ice for roughly a year, while in the meantime provisional trial runs were established in several member states. Outside the EU, a number of countries (most notably the US, but also Canada and Russia) made a push towards the implementation of body scanners. Moreover, Japan, Australia, South Korea, China and India announced that they were planning to purchase machines (Barros, 2012: 64).

Following the underpants bomber incident on 25 December 2009, however, several member states started to reconsider the use of body scanner technology, with the Netherlands emerging as the front-runner (Barros, 2012: 64). On 15 June 2010, with COM(2010) 311 final, the European Commission reported to the Parliament and the Council on the unresolved status of body scanners, summarizing the national experiences and calling for "a harmonised approach [that] should incorporate EU fundamental rights standards and a common level of health protection to allow adding this technology to the existing list of eligible equipment for screening persons at airports" (European Commission, 2010a: 2). In a report issued on 30 May 2011, the European Parliament supported the EC's initiative to harmonize the legal framework and the plan to include body scanners in the list of allowed screening measures at European airports. However, the Parliament made a number of claims concerning a possible implementation, "demanding to adapt the provisions on the protection of health, privacy, personal data and fundamental rights to technological progress" (European Parliament, 2011: 7). Specifically, the report called for an opt-out possibility from primary screening with body scanners, as well as the use of non-ionizing radiation in deployed devices. Moreover, the machines should rule out the possibility to store or retain images or data, especially not in connection with individual profiles. Most notably, the Parliament stated that "only stick figures should be used and [insisted] that no body images may be produced" (European Parliament, 2011: 9), but in general the report agreed to the European Commission's desire to implement body scanners on a regular basis.

Thus, on 11 November 2011, Regulation (EU) 1147/2011 eventually added body scanners to the list of allowed screening measures at European airports, updating the list provided by Regulation (EU) 185/2010. While the first three demands of the European Parliament had been adopted in the final regulation without revisions, the issue of 'naked' images of the human body remained unresolved. Regulation (EU) 1147/2011 leaves member states with the choice whether to implement machines that operate with a human reviewer or machines with privacy-preserving software that only display matchstick figures and that feature automatic threat object detection. In the former case, the human reviewer, located in a separate room, is still able to see the 'naked' body image and in case of detection of a forbidden object is set to communicate with the screening officer at the checkpoint, indicating the body parts on which to perform a manual secondary screening. Remaining irresolute on the delicate issue of privacy, the EU has thus passed the decision on how to deal with concerns of 'nudity' to the national level. Although EU legislation on aviation security has made considerable progress since 2002, the overall field still remains complex and unclear. As Barros (2012: 57) states, "EU, international organizations, states, and private companies are interacting in the global field of aviation security, which is far from institutionalized and structured", and in which body scanners have been used in a number of distinct ways.

Due to the federalist organization of the German state, 20 different public authorities and agencies are involved in the national level of aviation security (Giemulla and Rothe, 2008: 49). The national aviation security act (LuftSiG, 2005) distributes the responsibilities for security measures at German airports among three main pillars. Paragraph 5 entitles the Federal Aviation Authority to secure access to the airside area, including checkpoint operations and the decision on the deployed screening measures. At the majority of German airports, this task is enacted by the Federal Police which is formally subordinated to the Federal Ministry of the Interior. However, the Federal Police has the possibility to subcontract screening operations (LuftSiG, 2005: §5(5)), effectively leading to a situation in which screening operations are being carried out by private security companies. The two remaining pillars in the overall security framework address airport operators (LuftSiG, 2005: §8) that are obliged to protect the physical integrity of the airport, provide perimeter defence and ensure that screening can be carried out in an adequate fashion, as well as airlines (LuftSiG, 2005: §9) that are obliged to secure grounded aircraft and to ensure that only authorized individuals can access aircraft. After all, the security framework requires custom-tailored solutions for every single airport, as considerable differences in size, architectural style, available space and involved stakeholders do occur empirically.

Studying technology

An analysis of how security technology comes into being, as Guittet and Jeandesboz (2010: 236) note, has to carefully scrutinize "the diversity of groups of professionals who actually intervene into technological development, the overlapping arenas through which technological systems are funded, developed, marketed, promoted and acquired, as well as the multiple logics which underpin these processes." Setting the scope on body scanner technology, a complex assemblage of stakeholders has been involved in the process, coming not only from the specific aviation sector but also from the broader field of security. As Guittet and Jeandesboz (2010: 236) add, "one needs to distinguish between designers (e.g. engineers), marketers and promoters of technological systems, as well as between the agents responsible for acquiring technological systems (procurement administrations), for supporting research in the private and public sectors, and for using these systems – with the additional caveat that all of them intervene, through different arenas and interfaces, into technological processes."

The trial run at Hamburg airport was designed as a research project, initiated on the political level by the Federal Ministry of the Interior and enacted on the practical level by the Federal Police. As one Federal Police Officer put it: "It is not our own research project, but the research project of the Federal Ministry of the Interior, which has engaged the R&D department [of the Federal Police] with the task. We are just present at the airport and make our contributions, as a part of that research group [own translation]" (Expert Interview, 9 June 2011). This framing of the trial run reflects a securitization move as a long-term plan that includes research and development and the participation of the security industry. This way of cooperative implementation of security measures can be retraced at the European level as well. As de Goede (2011: 10) argues, "EU funding often prioritises this kind of precautionary and technologically advanced security research. The European Security Model is fostered through research funding and market integration." While on the EU level, this approach is realized in the Security Theme of the FP7 Framework (Bigo and Jeandesboz, 2010), similar structures can be found on the national level with the German Research Programme for Civil

Security (BMBF, 2007; BMBF, 2012). Funded by the Federal Ministry of Education and Research (BMBF), the program emphasizes the chances of security as an "innovation chain" (BMBF, 2012: 2), covering a long-term period from basic research to industrial design. Moreover, the initiative has fostered a special interest area of research on terahertz technology since the start of its high tech strategy in 2007 (BMBF, 2007: 102). As part of this strategy, the public sector made a push towards the industry in search of cooperation. As one representative from the security industry stated, public authorities had started to make inquiries to the industry following a number of significant terrorist incidents in aviation (Expert Interview, 12 January 2012). Since then, a number of projects (QPASS, TEKZAS, TeraCam, TeraTom, TeraHz-Videocam, TeraHz-Videocam TWO) from the area of 'Detection of Hazardous Objects' have targeted the development of body scanners and related applications to detect dangerous objects at security screening, often with a special focus on aviation.[8]

The industry reacted to this trend with the intensification of their own research agenda, while regularly checking back with the authorities. Said one expert from the security industry: "We have been constantly communicating with the authorities, we have been reporting to the authorities: What do you need? What is necessary? And so on. So we were informed about the authorities' plans, and they were informed about our activities [own translation]" (Expert Interview, 12 January 2012). The Federal Police itself has become an associated partner in the TeraHz-Videocam TWO consortium, enabling the authorities to closely monitor and advise research and development. As one involved expert said: "We see each other at project meetings, we have the possibility to straightforward call the R&D department of the Federal Police and to tell them: We have this or that idea, what do you think of it? Is that something you want to have? [own translation]" (Expert Interview, 15 March 2012). Thus, research and development on body scanners, funded by the government and in close cooperation with aviation security authorities, was progressing well in Germany. However, the turning point eventually came when the US Transportation Security Administration (TSA) launched images of 'naked' bodies to the media that had been produced by body scanners deployed at US airports in autumn of 2008. Originally meant to demonstrate the capabilities of the machines, the images lead to public outrage and broad debates about privacy and human rights not only in the US, but also in the European context (Abeyratne, 2010; Frimpong, 2011).

The security industry was taken by surprise by the events. As a representative from the branch said, their presentation of a new body scanner machine at the ACI Airport Exchange fair in Berlin, 27-29 October 2008, was severely affected by the pictures that at this point had been re-published by all major media outlets. Hence, he admitted that "[they] had to be more quiet than planned during the exhibition [own translation]" (Expert Interview, 12 January 2012) in order to avoid attention and critique. Added another expert from research and development: "Well, the debate had a lot of influence on us [own translation]" (Expert Interview, 15 March 2012). As a consequence, further efforts in research and developments took a turn towards privacy-preserving software solutions with automatic threat object detection, so no images of 'naked' bodies would have to be displayed any longer. Said one representative from the security industry: "With the neutral depiction, it is possible to dispel the rightfully uttered doubts. There is nothing objectionable about this matchstick figure [own translation]" (Expert Interview, 12 January 2012). But the turn to privacy-by-design soon revealed major hurdles in automatic image analysis. Algorithms that were found to work properly in a laboratory environment with predefined boundaries and parameters, indeed struggled to perform in a

[8] http://www.bmbf.de/de/12917.php (accessed 7 July 2014).

real airport environment. As one engineer clearly stated: “In my opinion, image analysis is not possible in an automatic fashion. Not with our current knowledge [own translation]” (Expert Interview, 15 March 2012). Regarding the developmental stages of image analysis and object recognition, another engineer added: “If you ask me about the time frame to realize such a system, I can’t give you a straight answer [own translation]” (Expert Interview, 14 February 2012). Thus, the security industry quickly realized that the respect for privacy issues had resulted in a system in which software turned out to be the weak link. The machines could distinguish whether an object had been found or not, but were not able to assess whether the found object posed a threat or was merely a handkerchief in a pocket. As one expert from a private security company put it: “It was easily possible to analyze the terahertz images, but with this artificial brake, that has become impossible [own translation]” (Expert Interview, 16 January 2013).

Thus, while on the political level, policy makers had efficiently tackled privacy concerns, body scanner technology itself had suffered a setback from the implementation of matchstick figures that replaced the original ‘naked’ terahertz images. From a research and development perspective, it became clear that airport environment testing would be necessary in order to make progress in automatic threat object detection. As one engineer admitted: “A trial run in a real environment is necessary to gain experience [own translation]” (Expert Interview, 14 February 2012). Accordingly, the trial run at Hamburg airport was eventually framed as a research project, but only confirmed what involved stakeholders had expected in the first place. Said a representative from the Federal Police: “Everyone from the R&D department, but also from the Federal Police, who knew what had happened in the laboratory environment, were pretty clear about what would happen during the trial run, and which problems would probably occur [own translation]” (Expert Interview, 9 June 2011). Since the machines were merely able to make a binary distinction between detection or no detection, the false positives rate was leaping up and manual secondary screening slowed down checkpoint operations considerably. As an expert involved in the trial run stated: “We are facing a high rate of false positives, caused among others by the software. One must not forget that we are enacting a trailblazer position here in terms of privacy with the pictogram solution, but at the expense of the scanner’s performance [own translation]” (Expert Interview, 9 June 2011). With regard to the decreased performance of the machines, a representative from the security industry added: “It is clear that the capacity of such systems is very important. Whoever buys such a machine is interested in as much capacity as possible [own translation]” (Expert Interview, 12 January 2012). So while from a research and development perspective, the trial run provided valuable experiences, the ensuing failure in terms of capacity eventually resulted in the numeric evaluation of the trial run and the non-deployment of body scanners in the German context.

Thus, privacy claims seem to have been surprisingly successful in the German context. And this success seems to be spilling over to other contexts as well. The US have also started to turn away from designs with ‘naked’ images. Mandated by Congress as part of the FAA Modernization and Reform Act of 2012, body scanners at US airports are set to feature privacy-preserving software, leading to similar problems in automatic threat detection. Rapiscan as one of the large manufacturers of body scanners at US airports has not been able to provide an adequate software for its machines in a timely manner. As a consequence, all Rapiscan machines are being removed from US airports and stored until the company can deliver the required new software version (TSA, 2013). Arguably, the success of privacy advocates in the case of body scanner technology might be due to the highly symbolic issues

of bodily integrity, shame and nudity that have been raised after the introduction of body scanners. Usually, civil rights are in a weak position when faced up against overwhelming security concerns (Tsoukala, 2010; de Goede, 2011), but in this particular context, privacy claims have prevailed in the struggle over a highly controversial new screening technology. While on the EU level, designs without privacy-preserving software have been allowed for national implementation, the German authorities have opted for the use of scanners with built-in privacy protection in the form of a software that does not depict the 'naked' body. However, this decision has eventually crossed a long-term securitization process, leading to the rejection of the machines, as they were deemed as not suitable for everyday use.

Conclusions

The aim of this paper was to analyze the question why body scanner technology has not been implemented at German airports, while it has been the case in the EU legal framework as well as in other member states such as the UK and the Netherlands. Going beyond the discursive level of speech acts, the paper sought to overcome the narrative chain in public discourse, which remained in plain numeric terms. Instead, the analysis applied a perspective that focuses on practices and professional knowledge from aviation security and the security industry. Conceptualizing the developments accompanying the implementation of body scanners in the EU legal framework and the (non-)implementation on the national level as a securitization process makes it possible to retrace very accurately how securitization in the German context failed. The securitization move was first initiated by the Federal Ministry of the Interior, emanating from long-term funding of research and development of terahertz technology that had been fostered by the Federal Ministry of Education and Research. The trial run of body scanner technology at Hamburg airport was itself framed as a research project, testing the capabilities and limits of a technology that had to be modified because of a number of public concerns, including privacy, data protection and health. Those issues were resolved on the political level, leading to the implementation of privacy-preserving software, which eventually resulted in major detection problems. Since automatic threat recognition software has not been able to keep track of the capabilities that body scanners theoretically provide, available machines turned out to be inappropriate for everyday use at the airport.

Turning the scope of securitization analysis towards technology itself, the very element that was set to be implemented eventually prevented a successful securitization process as it had to be adopted to changing political parameters. Public authorities as well as the industry had not estimated how privacy issues would ultimately unbalance the complex dispositif of aviation security in this case. Securitization in a Foucauldian understanding is not a straightforward process induced by powerful elites, but a dynamic and sometimes unpredictable development. Such an understanding can in terms lead to distinct policy outcomes and practices within the EU. As de Goede (2011: 16) notes, "indeed, a European security culture is not coherent and homogenised, but may be uneven, disjointed or even internally contradictory." Empirically, the European structures of enacting security through research funding and industrial cooperation can be found in a similar fashion on the national level. The German Research Programme for Civil Security (BMBF, 2007; BMBF, 2012) is focused on providing a long-term technological fix for the increasing number of national and international threats and uncertainties that have been identified in a post-9/11 order. On the EU level, the FP7 Security Theme enacts a very similar approach (Bigo and Jeandesboz, 2010; de Goede, 2011), thus raising questions whether the security agenda is fully being relocated

to the supranational level. While most notably the European Commission has pushed towards a European security solution at the expense of fragmented national frameworks (Kaunert and Léonard, 2012: 422), the German government has established parallel structures. Those structures have eventually fostered distinct developments in terms of privacy-preserving safeguards in body scanner technology, further contributing to an incoherent EU security framework. Turning the attention to the technological aspects within apparatuses of security, the analysis of a failed securitization process in the German context has shown that while on the legal level, privacy-by-design was the only claim that had not been fully implemented during the struggles over body scanner technology on the European level, the issue has eventually affected the field of aviation security from the bottom perspective of technology itself. Not only in Europe, but also in the US, recent developments have shown a tendency towards a built-in privacy approach that does not produce images of 'naked' bodies at all, but that instead depict privacy-friendly matchstick figures. As a consequence from this tendency however, the industry experienced an operational set-back, as automatic threat detection in image analysis turned out be a lot more challenging than expected.

Thus, it turns out that privacy claims have effectively foiled the implementation of new screening technology at German airports, preventing further intensification of security screening. Taking up Wæver's original notion of a normative desire for de-securitization, this actually seems to be a welcome change in a sector that is becoming increasingly dominated by new technologies and proactive approaches (Williams, 2011). As Wæver (1995: 56) emphasizes, "the trick was and is to move from a positive to a negative meaning: security is the conservative mechanism – but we want less security!" Recent developments in the European security agenda show a clear tendency towards relocating securitization agendas into the realm of research and development (Bigo and Jeandesboz, 2010). As technological tools are increasingly colonizing the realm of security, it becomes even more important to carefully scrutinize how complex assemblages are dominated and enacted by technologies, and how these technologies connect public and private agencies, policy makers, security professionals and the civil society. Further building on Wæver's (1995: 57-8) question what efforts could be undertaken to keep issues off the agenda of securitization or even de-securitize, the EU's as well as national scopes on research and development turns out to be problematic on a distinct level. As it is by definition a long-term process which is disconnected from the level of emergency and urgency that characterizes securitization moves within the discursive arena, its mechanisms are sometimes difficult to retrace. Research and development remain below public perception for a considerable time span before their outcomes eventually reach the surface of the public level, and by that time have often produced fully designed and market-ready tools. Given considerable time and resources, emerging technologies more often than not are going to realize their original goals. As one expert from a private aviation security company said: "When computing power increases, when the detection performance increases, and accordingly the false positives rate decreases – then the use of body scanners is definitely the right choice going into the future [own translation]" (Expert Interview, 9 June 2011). Securitization moves that stay below the original notion of exception and seek to intensify security or to converge once distinct competences pose some analytical obstacles. A closer look at how technology comes into being and contributes to securitization processes can provide help in understanding the European security agenda and thus should be an integral part of the still emerging research area on European internal security. In the case of body scanners, it seems that privacy-by-design could indeed spill over to other member states and lead to an ex-post failure of further securitization

in the aviation sector, unless technological progress on the software level catches up – which in fact could be expected to happen sooner or later.

[Inquiry 5]

Governing airport security: an empirical account between economic rationality and the public good

On a virtual trip through Toronto International Airport, as Rigakos and Greener (2000: 145) have pointed out, an occasional traveler "will have come under the gaze of three federal policing agencies, one municipal police service, a quasi-public security force, four privately contracted security companies, and an unknown number of in-house airline security agencies all working alongside one another." For more than three decades, scholars have now been concerned with the transformation of policing and the provision of security. But besides a shared insight that we have faced, and are still facing considerable change, the rise of private entrepreneurship and its impact on the governance of security have evoked distinct interpretations. While some have emphasized the chances of local and (partly) private forms of security governance (Shearing and Wood, 2003a), others have called for the re-establishment of a normative primate of the state in an area as delicate as the security of its citizens, and have doubted the beneficial regulatory capacities of the market (Loader and Walker, 2006). Airports as concrete sites for enacting international security have been deemed as spaces of "profound social and political significance" (Lyon, 2003a: 13) that not only provide global connectivity, but also "epitomize" the multitude of distinct relationships between public and private actors in the provision of security (Lahav, 2008: 81). Within a still emerging research agenda at the intersection of political and economic contexts (White, 2012), this paper seeks to contribute to an enhanced understanding of the mechanisms of security governance by providing empirical insight into practices at German airports. The out-contracting of security provisions in Germany is realized via a principal/agent setup that formally leaves a state body (the 'Bundespolizei') in charge of security operations, and thus stands in stark contrast to radical forms of privatization that can be found in other European countries, for instance in the UK. From this particular legal setup, a number of rather unique consequences emerge, thus rendering the case study fruitful for reflections about the relationship of the state and the market in terms of security provisions. The analysis lays its particular scope on screening operations at the security checkpoint, generally conceived as one of the most vulnerable spaces within the airport security framework (Jones, 2009), and claims that we can find major operational flaws in this specific mode of out-contracting, both alongside economic and political rationalities.

In order to closely examine the relationship between the police and private security companies at the airport, a total of 24 expert interviews with representatives from the aviation security branch – among them a considerable number of executives and staff from the private security sector – have been conducted from May 2011 until January 2013. Using this insider knowledge to create an account of German airport security, the paper finds that despite the overall security framework of modern airports is driven by neo-liberal economic rationalities, an overall approach of risk-management, and trends in technologies, the 'human factor' within this complex assemblage remains strangely neglected. Exposed to the regulatory mechanisms of the market through out-contracting, the private security companies that work the checkpoint face considerable economic pressure that effectively forces them to cut costs – and they do so primarily in staff expenses. As one representative from a private security company metaphorically described the situation: "Our role at the airport – well, one might frame this with the anatomy of the buttocks. One buttock is the Federal Police, and the

other buttock, that's the passengers and the airport operator. And the little brown thing in the middle, that's us"[9] (9 June 2011). It obviously seems a bit over the top to say that international security is enacted by scat, but the empirical insight indeed reveals how both economic and political pressures become re-located into the realm of private firms and their staff. Read through that lens, international security and its high-priority safeguards against major terrorist attacks such as 9/11 then boil down to the work and individual accountability of private security agents, whose work conditions have been criticized as inadequate (Lippert and O'Connor, 2003; Seidenstat, 2004). Thus, this conceptual shift to market regulation arguably undermines the expensive and technically sophisticated overall security framework of (German) airports.

Between necessary virtues and neutral nodes: security governance

Security and how it becomes enacted in contemporary societies has come a long way. Due to the legacy of the Westphalian system and its state-centric angle, thinking about security often carries a certain notion that the state has been responsible for, and in fact has been in charge of, the provision thereof throughout history. Yet still, the last couple decades have brought about a considerable change of the role of the state. This thesis of a recent "transformation of policing" (Bayley and Shearing, 1996) has been challenged, as others argue that new forms of security governance have not emerged only lately, but rather must be conceptualized as an ongoing phenomenon that can be traced way back (Jones and Newburn, 2002). However, scholars have been quite unanimous about the accelerated dynamics in this change and the rise of the private security sector. Empirical insights into the re-organization of police work and ensuing forms of "managerialism", "consumerism" and "promotionalism" that depict the commodification of security (Loader, 1999), into the emergence of new spatial setups such as gated communities and other forms of private property as well as hybrid spaces of "mass private property" (Shearing and Stenning, 1983) that are as often as not patrolled by private security companies, and into the changing dynamics of cooperation between multiple public and private security agencies have been along the major lines of inquiry. On a more general level, and alongside those tendencies, a shift from traditional repressive policing towards preventive, risk-based forms of policing (Ericson and Haggerty, 1997; Feeley and Simon, 1992) and an increased use or even lead of technology have been pointed out (de Pauw et al., 2011; Marx, 1988). Overall, the academic field of security governance across such disciplines as criminology, sociology, political science and the law appears as rich and numerous as security governance itself.

It is possible, however, to distinguish two major trajectories of theorizing the shift from a supposed state monopoly of security towards contemporary assemblages that consist of a multitude of both state and non-state actors. Mainly around the works of Johnston, Shearing, Wood and others (e.g. Johnston and Shearing, 2003; Shearing, 2006; Shearing and Wood, 2003a; Shearing and Wood, 2003b), a skeptical view towards state-centric provision of security has evolved. The state, in this reading, appears not a suitable primary actor for often delicate security tasks, as public authorities are often inflexible, bureaucratic and not particularly sensitive to the specific needs of distinct social environments. Thus, authors of this school argue that security as a public good can be enacted considerably better through individual configurations, for instance on the local community level (Shearing and Wood,

[9] All interviews have been conducted in German. Quotes have been translated by the author.

2003a). Moving away from a theoretical primate of the state then allows for an arguably better suited mode of empirical analyses. In an effort to scrutinize how state and non-state actors co-operate in distinct context, they propose to look into particular "nodes of governance" from an unprejudiced angle, thus ensuring that "no set of nodes is given conceptual priority" (Shearing and Wood, 2003b: 404) in any analysis.

A distinct reading of security governance builds mainly on the works of Loader and Walker (e.g. Loader, 1997; Loader and Walker, 2001; Loader and Walker, 2004; Loader and Walker, 2006), who conceive the state as a normative anchor of security provision in otherwise a-moral forms of governance that are increasingly determined by neo-liberal market imperatives. Despite being aware of the potential shortcomings of the state as a "meddler", "partisan", "idiot" or "cultural monolith" (Loader and Walker, 2006), scholars who follow this reading highlight the state and the democratic foundation, legitimation and direct accountability of public authorities as central elements in dispersed networks. This emphasis is based on the general notion that security and policing "represent a limit case of the freedoms and pleasures of consumption" (Loader, 1999: 387). The empirical findings of this paper indeed suggest that economically induced practices of out-contracting create working conditions that stand in stark contrast to a normatively founded account of security provision.

Subsequently, this paper argues that an 'anchored' conceptualization of security governance serves as a more adequate reading of practices of out-contracting screening duties at the airport. After all, "the need for economic regulation should be re-examined from time to time" (Starkie, 2002: 63) – or at least the relationship between public and private agencies should be re-evaluated. Such a re-evaluation necessarily must take into account concrete legal frameworks as well as ground-level practices. By looking both at how the particular German principal/agent setup of out-contracting has come into being, and through the analysis of expert knowledge from the field, this paper seeks to provide such an account, and to pin-point the normative and economic flaws of out-contracted airport security provision. Security governance at the airport, so it will be argued, could actually benefit in both normative terms as well as from the political rationale of effectiveness, if it was removed from the unmitigated regulative forces of the market. Before proceeding to the actual analysis, the next section locates the particular space of the airport and its characteristics among the axis between a state monopoly and the privatization of core aspects of security.

High-risk, low-cost hybrids

As several authors have emphasized, there is little conceptual use in dichotomous thinking about security governance either in terms of the state/the public or in terms of the economy/the private, when in fact numerous forms and constellations can be found empirically. As Dupont (2006: 87) points out, it appears more suitable to think of a "continuum approach, with the 'public' and the 'private' at each end, and various unpredictable combinations of pluralization and commodification in the middle." Thus, where does the airport locate among this continuum? The organizational structure of modern airports has been described as a "fragmented array of horizontal, vertical and lateral linkages" (Frederickson and LaPorte, 2002: 33), with a considerable amount of private service provisions, and particularly privatization and out-contracting of security tasks to private firms. Moreover, as Starkie (2002: 64) emphasizes, "airports, many of which have been treated in the past as public service organisations directly controlled by government administrations, have increasingly been restructured as public enterprises, or have been privatised." Thus,

airports fall in line with what Shearing and Stenning (1983) have deemed "mass private property." Those hybrid properties carry a strong notion of public space, but in fact are owned and/or operated by private companies. Prominent examples for such places are shopping malls and sports arenas, as well as transportation infrastructures such as train stations and airports. Especially the latter venues have been identified to operate between the public purpose of providing mobility infrastructure, and the need to generate economic revenue. In terms of security provision, private ownership carries considerable consequences. In some cases, public authorities remain in charge and as such govern private space, in other cases they cooperate and share/split tasks with private companies. More often than not, private policing even completely replaces public services, as most notably can be witnessed in shopping malls or sports arenas.

Along this notion of hybrid space, Rigakos and Greener (2000) have tagged airports as "bubbles of governance" that enact highly differentiated forms of security governance in order to be able to cope with the "myriad threats to social order" that create "myriad opportunities for the selling, trading, and contracting of security provision" (Rigakos and Greener, 2000: 146). Crucial for this understanding of bubbles is the notion that they represent spatial spheres which are governed by particular modes of public-private relationships. However, those relationships are relevant only within the bubble – once the individual leaves the bubble, they are no longer subjected to its mode of governance. Building on this very relationship of the individual with what used to be the state, but now consists of a multitude of public and private actors in unique constellations, Shearing and Wood (2003b) have used the term "denizen" to emphasize the changing constellations of governance that dominate everyday life contexts. Distinguished from the notion of citizenship, the concept of denizenship disconnects the fixed link to the state and rather refers to being governed through changing constellations of the public and the private. Individuals would then enter or pass through distinct spheres such as private homes, public streets, or hybrids such as malls or airports on a daily basis, and thus possess "multiple denizenships depending on the number of domains of governance through which their lives are regulated" (Shearing and Wood, 2003b: 408) – subsequently opening up a research agenda of how particular denizenships impact individuals and their conceptions of, and attitude towards the provision of security in distinct spatial constellations. A common argument from the aviation industry highlights the assumption that air travel should be regarded a voluntary option and that the entrance into the bubble of the airport and the acceptance of its particular denizenship would remain within individual agency. Thus, the purchase of an airline ticket would come with the mandatory requirement of subjecting oneself to security screening, and on a more general level with the notion that passengers would subject themselves to the overarching security regime based on a notion of space.[10]

While such a presumed voluntary nature of air travel in times of ultimate global connectivity appears highly doubtful, the security regime of the airport is in fact worth looking into. As "high-reliability organizations", airports have been compared with the likes of nuclear power plants or electricity transmission infrastructure (Frederickson and LaPorte, 2002). Such organizational forms can allow for no margin of error due to the potential catastrophic

[10] Such a notion of informed consent has been repeatedly expressed by representatives of the aviation branch, most notably at a conference on risk-based passenger security frameworks, Oestrich-Winkel, 15-16 May 2012, and at an NCAS workshop on "New passenger security concepts", Frankfurt, 25 July 2012. The author has been present on both occasions.

consequences in the case of failure of service provision. Thus, the scope for screening at the airport is on maximum security. The far side of the checkpoint has been described as a "sterile" space (Salter, 2008a: 13) that must by no means become contaminated by dangerous individuals and/or objects. In order to ensure this sterility of the airside area, airport security opts for the mitigation of risk. As the acceptance thereof is beyond question, and complete avoidance of risk (or, in other terms: absolute security) cannot be achieved, the mitigation approach has evolved as the most suitable operational mode for airport security. There are ongoing efforts to relocate the assessment and mitigation of 'risky' travelers to an early stage in both temporal and spatial terms (Leese, 2013; McLay et al., 2010; Salter, 2008b), but for now, risk mitigation at the screening checkpoint is enacted via physical scrutiny for dangerous objects and banned liquids. For this purpose, a considerable and ever-increasing arsenal of high-tech solutions that include full body scanners and trace detection for explosives offer assistance. Thus, airport security can be conceived of both in terms of risk-based and preventive approaches to policing (Lyon, 2006a; O'Malley, 2006; Salter, 2008b), and in terms of a strong innovation-centric account of security that strives to constantly implement the latest security technologies (Barros, 2012; Jones, 2009) in order to counter high-impact events such as hijackings and other criminal and/or terrorist incidents. This form of technology-led policing can in fact be described as part of a larger trajectory across many spheres of police work, but has arguably been reinforced in post-9/11 security efforts (Lyon, 2003a).

But while sophisticated and expensive technologies can serve as a capable supporting cast, the eventual decision whether to prevent any passenger from proceeding past the checkpoint remains within human agency. In case a potential security breach has been detected, manual second screening is set to determine the actual threat. Thus, security boils down to an individual decision, made under time constraints, as screening should not take up too much of the passengers' (shopping) time. It appears only reasonable that in an optimal scenario, this decision should be made by an experienced, well-trained and highly motivated screening agent. Thus, how can we make sense of the practice of out-contracting screening operations to private security companies, when prize competitiveness most likely negatively impacts the quality of the product – the provision of security? Scholars have intensely criticized out-contracting and private security provisions at the airport (Frederickson and LaPorte, 2002; Jones, 2009; Lippert and O'Connor, 2003), but little in-depth study of the nature of the public-private relationships in question has been conducted. The common position of critique might be summarized such that out-contracting relocates the provision of security into a highly competitive market environment in which the price is the dominant criterion and thus turns screening operations into low-cost labor. Ensuing consequences such as little organizational identity, inadequate job training and high staff turnover, so the argument goes, diminish the overall quality of security provision to a level that might actually produce security breaches and thus threaten international security. And while this argumentative chain appears widely accepted, there remains a need for empirical research that scrutinizes how airport security governance becomes enacted in specific assemblages of the state and the market. The next section seeks to establish such an empirical account. Or, put in different terms: "in gauging the impact of private actors on state sovereignty, we must consider who has been setting the agenda, who is delegating, and who is the agency" (Lahav, 2008: 95).

Out-contracting along economic and political contexts: an empirical account

Drawing on the notion that "political and economic processes and institutions are interlinked and should be studied as a complex and interrelated whole rather than as separate spheres" (Gamble, 1995: 517), White (2012) has suggested to set an analytical agenda for a "new political economy of private security" that unfolds along the dimensions of the political and the economic, but ceases to conceptualize them as distinct categories. In such an agenda, rather than reproducing traditional angles, "dichotomies between politics/economics, states/markets and structure/agency are consciously broken down and reframed within an integrated approach" (White, 2012: 86), thus allowing to think of security governance in terms of "private security providers as political economic actors moving back and forth within a political economic dialectic" (White, 2012: 96). Adding an explicit account of the economy to any analysis of security governance can provide not only a better understanding of the targeted question, but also provide an instrument of critique. Not least of all, economic analysis has the potential to identify market failure and thus justify intervention (Ogus, 2004: 31), thus serving as an additional layer besides normative forms of critique.

Historically speaking, the emergence of security governance at German airports can be retraced to changes in the legal framework of aviation in the 1990s. The provision of security at airports has in fact traditionally been a monopoly of the state throughout most of Europe. Towards the end of the 1980s, however, and due to the ever-increasing numbers of flights and passengers, authorities slowly began to conceive of their tasks in more economic terms. As Ericson (1994: 171) points out, during this period governments began to realize that "there are finite resources that impose limits on security provision" and thus searched for new and more cost-effective ways of policing the aviation sector. The 1988 UK aviation deregulation act has been deemed a trail blazer towards a wave of privatizations across European airport security (Hainmüller and Lemnitzer, 2003: 9). However, German authorities remained skeptical and reluctant to the potential outsourcing of security tasks. It was only in 1990, "when budget constraints of the state made changes in the distribution of the financial burden seem inevitable" (Hainmüller and Lemnitzer, 2003: 11), that political action was undertaken. Subsequently, an aviation security fee was introduced in order to compensate for costs in terms of personnel and expensive screening technologies such as metal detectors. However, airport security remained within the realm of the state for the time being. By 1992, out-contracting of screening operations eventually became a legal option, but it was only in 1995 that screening operations were eventually carried out by a private security company for the first time, with the airports of Stuttgart and Hamburg being the frontrunners for this new mode of security governance. The choice of out-contracting over outsourcing has prevented a complete turn towards privatization, though, and has led to the principal/agent setup still in place today.

Since then, out-contracting of checkpoint operations has become a standard procedure at German airports, the renewed legal framework for which is provided by the Federal Aviation Act ("Luftsicherheitsgesetz", LuftSiG, 2005). According to §5, the Federal Police ("Bundespolizei") is in charge of screening operations at most German airports.[11] However, the police as security provider are entitled to out-contract most of their actual tasks, as long as they retain a supervisory status at the checkpoint (LuftSiG, 2005: §5). Thus, with the

[11] Due to the federal organization of the German state, in some cases state or local police authorities are assigned with this task (Giemulla and Rothe, 2008). At Munich airport, for instance, the Bavarian State Police ("Bayrische Landespolizei") is in charge of the screening operations.

exception of core statutory powers such as identifying or detaining individuals, private companies are eligible to execute what might be described as 'police work light'. Or, in concrete terms: searching passengers and carry-on luggage for dangerous and forbidden objects, but referring to the actual police in case further action has to be undertaken. The role of private security companies in this relationship might thus also be compared to 'deputy sheriffs'. As one interviewee put it: "We are just the first wave. We detect, and then we notify. That's it. The very moment a conflict arises, problems occur, we pass the torch. That's a matter for state authority then, that's what we have it for" (9 June 2011). Osborne and Gaebler (1993) have famously described such constellations as "steering/rowing", with the state steering at a distance while the rowing work is executed by other (private) agencies.

In terms of the quality of policing, Hainmüller and Lemnitzer (2003: 22) have argued that in such principal/agent relationships, the provision of security performs considerably higher than in genuine privatization environments, as "due to the right institutional incentive structure (rigid monitoring and powerful sanctioning), the regime is still compatible with the security goal." In their analysis of German airport security, they thus come to the conclusion that Europeans fly particularly safe, especially compared with the US system before the federal Transportation Security Administration (TSA) was founded as an institutionalized reaction to 9/11. However, while there are good arguments for the performance of principal/agent setups on the theoretical level, this paper claims that on the empirical level, quite the opposite can be found. Considerable problems emerge from the practice of out-contracting that might eventually render the human factor – arguably the weakest link in the socio-technical assemblage of airport security – even weaker. Following an analytical agenda of new political economy, those problems can be located along the interlinked dimensions of the economic and the political. The former, as will be argued, triggers a causal chain of high competition and ensuing low wages in the private security sector, leading to an inadequate pool of workforce, high turnover and subsequently little long-time expertise. Arguably, this is also the reason why job training for screening duties at the airport is kept to a minimum. Along the latter dimension unfolds a number of issues related to democratic legitimization and accountability. With practices of out-contracting, responsibility for security breaches is relocated to the individual level, where it can be retraced to the failure of particular screening agents, and further reinforces pressure on an underpaid workforce. Thus, political and economic contexts combined appear to stand in stark contrast to the provision of security as a public good and provide adequate reason to question the current governance of airport security in principal/agent setups.

Economic trigger, causal chain

Due to legal provisions, the Federal Police are obliged to invite tenders for screening contracts every five years. Bids from private companies have to include, among others, concepts for job training, implementation, quality control, networks and communication. However, as one representative from a private security firm clearly puts it, "the price is a killer criterion" (8 November 2012). Moreover, not the Federal Police themselves are in charge of the decision which private company might be best suited for the job, but the decision lies within a federal procurement office which, due to the lack of expertise in the field of security, is likely to judge by the solid number that is the overall price for the offered service provisions. In fact, as admitted by several interviewees, other factors will regularly be trumped by budget arguments and the contract will eventually be awarded to the lowest bid. And while this

market-based mode of price regulation might in economic theory indeed lead to more cost-effective services, the private security sector tends to struggle within such a highly competitive environment. After all, the provision of security remains a high-reliability task that requires adequate resources. However, price dumping has evolved as a common strategy, sometimes deliberately used to break open new business opportunities. As argued by a representative from a private firm: "You can always say: OK, we really want this contract, this is a matter of prestige. And then you say: OK, then in this case we won't make a profit, but we will accept a loss" (8 November 2012). Those factors combined have on the one hand led to a considerable number of bankruptcies, and on the other hand have severely affected the image of the private security sector. Said one respondent: "Quality is expensive, and we all know that this is true for security and security firms. But one also has to say that at least in part this is the private companies' own fault. They have ruined their reputation in the context of public tenders and dumping offers" (8 November 2012).

Just as well, this negative image is due to the low wages in the private security sector. Interviewees unanimously stated that staff expenses are the most effective adjustment in order to be able to compete in aggressive bidding environments. As one interviewee pointed out: "To be fair, one has to admit that this is a sector that does not pay well. In my opinion, there is a clear discrepancy between job specifications and payment. I find this quite remarkable, I mean the employees are really struggling to maintain a regular standard, financially speaking" (31 May 2011). Certainly, not all private firms are willing to cut even deeper into the expenses for their workforce, but even those who refuse to do so have to admit that their wages are comparably low. Said one executive from a private security company: "There are a lot of tenders where we have to admit that we are too expensive. But I mean, you can't really save money by cutting costs for personnel. They have to live off of something, and they are not well paid anyway. If you cut into that – that is just impossible" (8 November 2012). This spill-over of market rationalities into the security domain has been criticized both from organizational and normative angles. The normative claim here goes beyond the standard argument for adequate pay and working conditions. Alongside privatization and out-contracting runs a particular mode of shifting responsibilities "to a newly constituted, insecure working population and, in so doing, to externalize the risks associated with changing market demands and unstable future funding levels" (Lippert and O'Connor, 2003: 340). In case of a security breach (either a real one, or as part of a "real test" carried out by the Federal Police), individual responsibilities are in fact retraced to the individual screening agents in duty at the point in time, and disciplinary consequences range from additional training up to termination of the contract. This rather political question of democratic legitimation of security provision and accountability of private companies will be taken up again in the next section.

But considerable critique has also been uttered from an organizational perspective. While "contracting can work well when there are organizations skilled in providing the services needed" (Frederickson and LaPorte, 2002: 39), this particular skill largely depends on available financial and human resources (Frederickson and LaPorte, 2002: 36). As has been shown, bidding practices put considerable constraints on the availability of sufficient financial resources. From there, a direct link can be drawn to an apparent lack of adequate human resources in airport security. As one respondent pointed out: "Who applies for those jobs anyway? Half of the employees in the security sector comes straight from the employment office. That shows the level which we operate on" (8 November 2012). And while from former unemployment no lesser job performance can be extrapolated, such arguments have been

put forward during several interviews. Moreover, this particular characteristic has arguably been reinforced by the mode of job training within German airport security. Screening agents ("Luftsicherheitsassistenten") are not required to complete a regular two or three year job training, as is the case for many other professions in Germany. On the contrary, their training is provided by a mere multi-week training course with an overall volume of 160 hours. The training course framework and its contents are determined by the Federal Ministry of the Interior, but the actual training courses are carried out by the private firms – and this is what makes them a popular target for the employment offices. Low level qualification requirements and in-house training qualifies the private security sector as a fashionable opportunity for the state to attract and retain citizens in employment.

Thus, formerly unemployed applicants for screening duties at the airport receive considerable financial support from the employment offices – which is paid directly to the private security firm. Said one executive from a private company: "Those are the candidates they send to us for applications. And in order to ensure that we accept them, the employment office lures us into it by paying for the job training" (6 June 2011). One might indeed be inclined to say that those are not the best starting grounds to obtain a qualified and motivated workforce. As another executive added, "payment takes care of the rest. With this level of wages you only attract certain levels of society" (4 December 2012). Thus, working conditions and low wages in the security sector considerably reduce the pool of potential employees and arguably impact the quality of security service provision. As admitted by a private firm executive: "It is difficult to make a general statement here, but one can observe that the quality of the employees has not been increasing over the last couple years, but rather decreasing" (4 December 2012). After all, as Lippert and O'Connor (2003: 339) emphasize, "one can cost-cut and downsize only so far; beyond a certain point, organizations fail to produce or perform service functions."

Or so the common argument goes, at least. But do underpaid employees necessarily produce lesser performance results? It would in fact appear short-sighted to equate inadequate working conditions and payment with inadequate quality of security. As one interviewee points out: "I believe a screening agent is an expert for their job, and that is to produce security. And I would claim that they know how to handle their tasks, and that they handle them well, and that there is no reason to believe that the same screening agent would do a better job if they were employed by the state" (20 December 2012). This is obviously a valid objection. The initial problem of supposed low levels of service becomes clearer, though, when looking at the level of staff turnover the private security sector has to cope with. For the Canadian context, Lippert and O'Connor (2003: 343) have pointed out extremely high turnover rates in out-contracted airport security screening between 121 and 300 percent per year, and numbers for the US context vary from an annual average of 126 percent up to peaks of 416 percent at single airports (Seidenstat, 2004: 281). The reasons for this level of turnover arguably lie in structural limitations of the sector, such as "little chance for improvement, lack of adequate training, tedious and boring work, and other job-related factors" (Seidenstat, 2004: 281), that put severe constraints on long-term career perspectives within airport security. Not surprisingly, interviewees have repeatedly pointed out that many employees merely view a job in the private security sector as a short-term, transitory option. As one respondent framed it: "Today, within private security companies, we have a lot of people, especially those who came from the employment offices, who are really glad to have a job again. But the minute they can find something better, they will be gone in the blink of an eye. That means you'll have a high level of turnover. And that is not to say that turnover is high

because people don't like the job. On the contrary, many do like the job, and the flexible working hours – a lot of them actually do like working shifts – but they can just step up financially after two or three years, and they take that opportunity. As a consequence, within the private security sector, you merely have anyone who sees the job as a long-term career path and carries it out for longer than five years. Thus, you are stuck in a tread-mill and this creates a whole new level of training expenses, because you constantly have to train new people" (8 November 2012). Arguably, this is a major reason why the required job training for screening tasks at the airport contains a mere 160 hours. Turnover transforms the sector into a steam machine that constantly needs new fodder in order to maintain its operability. On the downside, however, the ensuing lack of adequate training raises major concerns. As one expert put it: "It's an extremely responsible job that demands a lot from the employees, also in terms of concentration and thoughtfulness. It's more or less a short-term training course job, although with an exam at the end. But with one month of job training, I'd be let loose on mankind in order to produce security for thousands of passengers" (6 June 2011).

This quote fairly summarizes the multiple dilemmas private security providers at the airport appear to be stuck in. They have been reconstructed as a causal chain that had been triggered by the liberalization of the European aviation sector in the 1990s. Alongside the commodification of airports themselves and their ongoing transformation into global shopping malls with terminals attached to them, the provision of security appears to have suffered from such an approach. This is not to say that the current system would not work – but despite being kept on a short leash in the current principal/agent setup, private security is generally regarded to be more prone to operational failure due to budget constraints, even when under a managerial supervision. Thus, the economic context of the analysis appears rather bleak. However, as pointed out, such a one-sided analysis appears hardly adequate to the complex set of questions that emerges from structures of security governance along the public-private continuum. As Salter (2008a: 23) emphasizes, it is important to "measure not simply the economics or business cases but also the democratic and social implications of new modes of control and facilitation." Or, as Loader (1997: 386) states, the organizational flaws pointed out in this section might indeed be overshadowed by a "wider, more diffuse unease about permitting market imperatives to determine the distribution and accountability of policing and security." Thus, the next section addresses questions of political rationalities, dealing with issues of security as a public good, democratic legitimization and the relocation of responsibilities into the realm of the individual.

The political context and the public good

Large parts of the debates in security governance are concerned with questions of transformation processes and actor cooperation in policing. Within this context, several authors have pointed to a general uneasiness with security provision that is regulated within a purely economic mode (Loader, 1997; Loader and Walker, 2006; Zedner, 2006a). In a normative reading of security as a public good, indeed "there is something about security that means its provision cannot simply be left to the unfettered market" (Loader, 1997: 383). With security being a good that benefits society as a whole as much as its individual members, its provision then becomes connected to the overarching societal framework and subsequently to questions of political legitimacy and the state. Public authorities as agencies of the state are not bound by the constraints of an economic agenda that would distract them from security tasks – at least in an ideal world. But as has been shown, finite financial resources

have been the very cause for the state to out-contract security provision at the airport and to become a consumer rather than a producer itself. Thus, what are the consequences of different actors carrying out classical police tasks? Arguably, the difference can be found in distinct modes of accountability – not so much in legal terms, but in terms of direct legitimation of public authorities and the lack thereof in the private sector.

As pointed out by Shearing and Wood (2003a: 216), "those who 'act publicly' act in ways that are accountable. In this vein, 'private acts' do not call for accounts or justifications of past actions. This is so because private actions are seen as furthering private interests, and as such are not usually a public matter." The state, and subsequently its institutions – in this case the Federal Police – are expected to operate strictly alongside their pre-determined and transparent agenda. The police are to provide security. And if they fail to do so, they must present themselves accountable towards the citizens. What we find in this ideal typical connection is a direct link to citizenship and its role in the constitution of the state and the public sphere. However, recalling the notion of denizenship introduced earlier, individuals today are rendered subjects of changing forms of security governance that depend on the respective spatial context. As will be argued, the particular mode of out-contracting at German airports re-locates responsibilities and accountability not only into the realm of private firms, but eventually even into the realm of the individual. Thus, while private security providers at the airport find themselves confronted with very limited possibilities of flexibly managing their workload due to strict contractual requirements, the Federal Police themselves have withdrawn from being responsible for actual concrete security breaches.

The deputy status of private security firms in the principal/agent setting at the airport is institutionalized in a hierarchical order. The Federal Police not only remain in charge of all statutory powers and critical decisions, but even become involved in the private firms' internal organizational processes. What Hainmüller and Lemnitzer (2003: 12) have called a "rigorous institutional straightjacket" goes in fact as far as setting up work schedules for the private screening agents. Said one representative: "The private firms don't have any choices in the organization of screening operations. They have to meet the exact requirements of their customers. Everything is regulated so specifically that the only thing open for decision remains the color of the uniform and the tie. Everything else is determined from the customer's side. This means very little flexibility for managing work schedules" (4 December 2012). This critical stance mirrors the top-down hierarchy that is being exercised within airport security. One expert indeed went as far as to claim that this hierarchy was a legal misconstruction: "There is a construction flaw in paragraph five of the aviation security act. The flaw is that the Federal Police have the operative responsibility. […] They in fact run the private security company, arrange work schedules, assess the strengths of the employees and so on, although they lack the expertise for this task" (8 November 2012).

Police work, as Ericson (1994) has pointed out, consists for a large part of the management and distribution of expertise and knowledge. However in the case of airport security, this knowledge is neither adequately transferred to the private sector during job training, which is set up by the Federal Ministry of the Interior, nor does it (positively) impact the everyday work of private screening agents. In a regular screening operations setup, only few Federal Police officers are physically present at the far side of the checkpoint, and are to be called upon in case conflict arises and their statutory powers become necessary. Apart from that, the role of the Federal Police is pretty much reduced to organizational tasks – for which, in contrast to actual policing, they have little skills. This fall in fact in line with Loader's (1999: 375) analysis

of increasing police "managerialism", only that the shift towards more business-like structures in this case does not target the internal structure of the police organization itself, but rather the internal structure of the private security provider. Organizational intervention is not the only impact of the police on the private sector, however. In order to exercise quality control, a system of audits has been established to ensure that contractual obligations are adequately executed. Said one interviewee: "Those processes are audited on a regular basis. And after each audit we can see that the screw has been severely tightened. This goes on and on in waves" (20 December 2012). Within highly commodified and privatized environments such as airports, audits enact an important function as numeric and quantified interfaces between the public and the private sphere. As Shearing and Wood (2003a: 216) have noted, the "audit as a technology has also been associated with the rise of 'business planning' processes, where devolved state authorities and providers set targets and render themselves accountable, in a future-oriented manner, for achieving these targets."

Thus, instead of the original chain of accountability that runs from the public authority to the citizen, out-contracting has added another layer. The chain now involves a series of accounts from the private firm to the public authority and from there to the (temporary) denizen. However, when looking more closely into how private security companies are managed by the Federal Police, it becomes clear that there is yet another layer to be found: individual responsibility. Apart from regular audits, the Federal Police also carry out so-called real tests, in which unknown persons, equipped with dangerous and forbidden objects, are sent through the checkpoint in order to determine whether they would be detected or not. As indicated above, consequences in the case of such a virtual security breach are severe. And more particularly: they are individual. Said one interviewee: "Real tests put the employees under a certain pressure that they are always attentive and always have to be attentive. Because they always have to reckon with somebody who carries something. That is the reality, after all. Whether this measure is appropriate, that is open for dispute. But tests are conducted on a regular basis, and then you have external people who carry something and hopefully they will be detected. […] And if they are not detected, we are obviously notified. As soon as one object is not detected, the employee has to undergo additional training. […] Then there will be a report, saying employee X has missed this or that" (8 November 2012). To clarify the dimensions of individual responsibilities, Salter (2007: 56) has pointed out that a screening agent at middle-size Ottawa airport in Canada carries out more than a million security decisions per year. And each one is a potential real threat as well as a potential test that enacts quality control on the individual level. Thus, a large amount of pressure is being put on the individual employee. Arguably, this pressure does not exactly contribute to enhanced working conditions.

The political rationale behind the out-contracting of security provision at the airport has not exclusively driven by the desire to cut costs, but arguably also by a desire to introduce additional layers into the once direct accountability of police work towards the citizen. In case of a security breach, blame is unloaded on the individual screening agent, and to its private employer that has failed to comply with contractual obligations. Only after those two layers have considerably dampened the harm of the possibly severe consequences that an attack on the target of aviation can carry for international security, the police retain a mere symbolic form of accountability. Framed in Osborne and Gaebler's (1993) terms: when steering to port, but the rowers turn to starboard instead, auditing mechanisms might have been insufficient and the organizational screws might not have been tight enough. The crucial point, however, is that the Federal Police have abandoned their core task of policing in favor of managing along

a neo-liberal agenda that has freed them both from budget constraints and from the chores of actually producing security. However, as has been pointed out throughout the analytic account of security governance, this conceptual turn has come with a price tag. Negative consequences have become imposed on an underpaid, undervalued workforce, and ultimately on security as a common good itself.

Conclusions: "more state, please"?

This paper has located German airport security among the public/private continuum of security governance, analyzing how both political and economic rationalities have been combined into a principal/agent setup that frees the state from monetary and democratic pressures. Public tenders and ensuing bidding practices have in fact created severe financial constraints for the private security companies that carry out screening tasks, while on the political level, the accountability chain towards the citizen has been transformed and prolonged, adding additional layers to the link between denizens and airport security. And while the state from a formal perspective indeed remains the anchor in the principal/agent setup, the question arises whether the anchor has deliberately closed its eyes? Despite retaining supervisory status in the actual operation of the checkpoint, the Federal Police have not only out-contracted the rowing, but have out-contracted all the chores of having to deal with job training, working conditions and staff turnover. And more importantly, out-contracting, while originally conceptualized as a policy tool for money-saving, has put severe financial constraints on the provision of security. Thus, which conclusions can be drawn from the empirical analysis? The German principal/agent model appears to be stuck between the notion of the state as the principal security provider and the commitment to fully-fledged privatization. At the same time, this particular setup seems not to solve the initial problems considerably well, but rather produces new problems. On the one hand, the state and its authorities have (deliberately) lost their direct accountability, and on the other hand, organizational constraints effectively hinder the unfolding of market self-regulation, as could be expected from true privatization.

What to make from this rather harsh judgment, then? Facing the choice of whether leaving the provision of security to the unfettered forces of the market, or whether re-locating it back within the realm of the state, the latter option appears the morally right one. The state within airport security might indeed be better suited as a true normative anchor than as the organizational anchor in the current principal/agent setup. As a directly legitimized "necessary virtue" (Loader and Walker, 2006), public authorities have the capabilities to not only remedy unease towards market imperatives of security provision that do not necessarily represent the public interest (Loader, 1999), but also possess the capabilities to fix the apparent shortcomings of the current setup. The analysis along the trajectories of the connected contexts of the political and the economic has shown that the "question of whether any substantial transfer of authority to the private sector should be permitted without adequate safeguards for public protection" (Zedner, 2006a: 273) in the case of airport security should indeed rather be answered with a 'no'.

In conducting an analysis of the organizational shortcomings deriving from the implementation of economic rationalities into the policing of German airports, the economic agenda itself then can "be used to indicate what sacrifice would have to be incurred, in terms of aggregate social welfare, in order to achieve the given distributional objective" (Ogus, 2004: 35), and thus complements a normative argument that unfolds along the re-location of

accountability for security provisions and the failure thereof into the realm of the private and the individual. Or, as Dupont (2006: 104) has framed it, “the power struggles and corporatist interests that fuel them contribute little to the optimization of security as a public or common good.” Reading security as a public good that benefits all members of society might in fact also require the commitment to carry a heavy workload for the realization of that goal. In other terms, it might mean that the state and its institutions would be obliged to row themselves, instead of just using the metaphorical microphone to shout out to the private security sector and tell an insecure workforce in which direction and how fast they are to row. To conclude with the now famous claim by Loader and Walker (2006: 167): “the state’s place in producing the public good of security is both necessary and virtuous.”

[Inquiry 6]

The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the EU

Data-driven analytics as a new practice of knowledge creation are on the rise – and not only in economic contexts. Reinforcing a general tendency of post-9/11 security policy making, the EU has recently fostered trends in intelligence collection, analytics and predictive data mining. The Stockholm Programme as the Council framework for the period of 2010-2014 formulates clear goals for "upgrading the tools for the job" in terms of data sharing and interoperability of databases in order to better enable law enforcement agencies to tackle terrorism and serious crime (European Council, 2010: 18-9). This trend has led to an increasing number of policy initiatives related to large amounts of information and the governance of future contingencies. As Geyer (2008: 1) summarizes the ongoing developments, "new ideas and proposals intending to allow public authorities to gather, store, process and exchange an increasing amount of personal data are being brought forward in high numbers and with increasing frequency." European systems like the Schengen Information System (SIS I + II), the Visa Information System (VIS), and the pending EU Passenger Name Record (PNR) Directive seek to collect and combine large amounts of personal information from mobile populations in order to scrutinize and assess the individual and the risk it possibly poses. Thus, data is rendered as a major asset in the fight against terrorism and transnational crime. The use of risk as a means for making the future actionable in terms of security governance has in fact become a rather ubiquitous measure, targeting wide-spread areas like insurance (Lobo-Guerrero, 2011), the financial system (de Goede, 2008b), border control (Amoore, 2006; Muller, 2009; Salter, 2004), catastrophe and disaster management (Anderson and Adey, 2012; Martin and Simon, 2008) and large-scale events (Boyle and Haggerty, 2012), as well as international transportation (Lyon, 2006a; O'Malley, 2006; Salter, 2008e). However, a series of questions emerges from the notion of risk and anticipatory governance. As Anderson (2010a: 778) puts it: "how is 'the future' being related to, how are futures known and rendered actionable to thereafter be acted upon, and what political and ethical consequences follow from acting in the present on the basis of the future?"

This paper engages with the still pending EU PNR Directive that is set to be one of the cornerstone policy tools of the Stockholm Programme. The system envisages, among other things, to make use of passenger data as a means to create new criteria for the identification of terrorist and transnational criminals and thus serves here as an empirical example for broader shifts in knowledge creation that the paper looks into more closely. Distinguishing between traditional profiling that performs confirmatory structure testing operations ('deduction'), and new and data-driven forms of profiling as a way of structure exploration and knowledge generation ('induction') (Anrig et al., 2008: 66), it will be analyzed how different modes of scrutinizing mobile populations enact distinct modes of governing. It will then be shown how these modes are reflected in the so-called "real-time" and "pro-active" approaches to processing PNR data (COM(2011) 32 final: 3-4). While "real-time" use essentially enacts traditional profiling practices, the "pro-active" concept, as detailed in the proposal, explicitly aims at "analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments" (Art. 4, 2(d)), thus establishing the prerequisites for making sense of large amounts of information via algorithmic exploitation and the data-driven creation of profiles as temporary hypotheses (Hildebrandt, 2008: 18). Connecting the findings

to Foucauldian thought on modes of governance eventually enables the analysis to demonstrate how new modes of knowledge creation impact the re-assembling of elements within apparatuses of security, empowering temporary and 'mobile' hypotheses of suspicion and at the same time disabling static types of anti-discriminatory legal instruments.

Most scholars that engage with PNR data concentrate on issues of privacy and data protection (de Hert and Bellanova, 2011; Bellanova and Duez, 2012; Bennett, 2005). However, with respect to security, governance based on algorithmic analytics raises a number of issues that are seldom addressed by the social sciences. Excellent contributions to understanding profiling often remain on a theoretical level (de Vries, 2010; Rouvroy, 2013), tackle legal issues (Brownsword, 2008; Zarsky, 2011) or shed light on commercial sector practices (Gandy, 1993; Gandy, 2010; Cheney-Lippold, 2011). This paper thus seeks to re-connect theoretical insights into profiling with empirical evidence from EU security policy making and thereby to offer a conceptualization of the changing landscape of security governance. It concludes that with the ongoing emergence of data-driven profiling, the legal toolbox of the anti-discrimination framework suffers an increasing ineffectiveness. Due to dynamic algorithmic systems, possible cases of discrimination will be less visible and traceable, leading to diminishing accountability.

Aviation, risk, and PNR data

The aviation sector has been framed as a particularly perfect fit for anticipatory governance, both for its highly symbolic role in the attacks of 9/11 and the ensuing 'war on terror', and for the applicability of the concept of risk in checkpoint-centered screening operations (Leese, 2013). In the spatial bottle-neck of the checkpoint, the passenger flow becomes slowed down for the purpose of thorough scrutiny and access regulation to the secured sectors of the airport (Jones, 2009). The deployment of risk profiling in this context promises to enact preemption in terms of re-allocating screening resources to 'risky' individuals, while facilitating travel for low-risk profiles, and at the same time increasing cost-effectiveness (McLay et al., 2010). Specifically in aviation, screening policies necessarily must aim at minimizing Type II errors (false negatives), as an individual that was incorrectly assessed as harmless while being a potential offender poses the worst-case scenario and could cause devastating harm. Thus, risk assessment at the airport must be very rigid and is subsequently prone to produce exceptionally high numbers of Type I errors (false positives). This caveat is also referred to as the base-rate fallacy problem of security measures that have to deal with an overwhelming majority of 'normal' cases and therefore are not resource-effective (Cavusoglu et al., 2010). However, there are a number of real-life consequences for being incorrectly flagged as a high-risk individual in security regimes, resulting in intensified and potentially invasive control at all stages of mobility. Contextual factors in security operations moreover amplify the chances of being singled out from the passenger flow and being further scrutinized, both due to time constraints on the practical level and a dichotomous logic of suspicion/non-suspicion in security screening.

Yet still, on several recent occasions, representatives from the aviation sector have called for more risk-oriented security policies, as for instance during the EC's High Level Conference on "Protecting Civil Aviation Against Terrorism"[12] (European Commission, 2011c) and the ICAO's (International Civil Aviation Organization) High Level Conference on Aviation Security[13] (ICAO,

[12] Brussels, 27 September 2011.
[13] Montréal, 12-14 September 2012.

2012). From an industry point of view, both the International Air Transport Association (IATA, 2011) and a joint venture of the Airports Council International and the Association of European Airlines (ACI/AEA, 2011) have presented concepts that seek to translate advanced passenger profiling into concrete screening procedures. Moreover, the aviation sector remains a key topic on the current political security agenda. Being mandated by the Stockholm Programme (European Council, 2010: 19), the establishment of a European PNR system is regarded one of the most important policy tools in fighting terrorism and transnational crime to be implemented until 2014.

Such an EU PNR system has a long history by now, and its status remains unresolved for the time being. The Commission's original proposal from 2007 (COM(2007) 654 final), already agreed upon by the Council, had been thwarted by the entry into force of the Lisbon treaty and the ensuing Treaty on the Functioning of the European Union (TFEU) on 1 December 2009, resulting in the dissolution of the pillar structure. However, as PNR data was considered a major factor in providing much-needed information for fighting terrorism and serious crime as well as for border control and migration issues, the Commission presented a new proposal on 2 February 2011 (COM(2011) 32 final). On 23 April 2012, the Council also presented a further advanced proposal (8916/12). The Commission's proposal was eventually forwarded to the Civil Liberties Committee (LIBE), which rejected it with a vote of 30 to 25 on 24 April 2013.[14] Despite this rejection, however, the Commission quickly pointed out that the vote was merely a committee vote, and that adoption of the proposal still remains high on the agenda, as it is considered extremely important and urgent.[15] The fact that an European PNR system is regarded as one of the core policy tools in the Stockholm Programme, as well as the persistence of the Commission with regard to the proposal render it possible that a (revised) version of the proposal could be decided upon in a plenary vote in the Parliament, thus increasing the chances for an adoption. In any case, it appears likely that the plans for such an EU PNR system will not be crossed off the agenda easily.

What makes PNR data so valuable, then? Originally used for the commercial purposes of airlines, PNR files contain large amounts of data that are obtained automatically during booking, reservation and check-in – for instance the name of the passenger and their address and full contact information, forms of payment including credit card information and billing address, the complete travel itinerary and the travel status as well as frequent flyer information (Council of the European Union, 2012: Annex II). Thus, almost naturally, PNR data has drawn interest from public authorities. As de Hert and Bellanova (2011: 4) state, being "one of the most detailed and personal data sources, it has gained enormous symbolic and practical significance in the debate about data sharing, and has been the subject of several international agreements, national measures, political and institutional clashes, as well as strong academic interest." In fact, PNR data as such have been collected by air carriers for handling bookings, flights and consumer information long before the first EU PNR agreement with the US on 28 May 2004 (with subsequent agreements in 2007 and 2011) has turned the data into a resource for security operations by the US Department of Homeland Security (DHS), and has made PNR data the topic of broader public discussions. The European PNR Directive, similar to the EU-US agreement, is set to cover all flights from the EU to third countries and vice versa, possibly leaving member states with the option of an additional opt-

[14] http://www.europarl.europa.eu/news/en/news-room/content/20130422IPR07523/html/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal (accessed 7 July 2014).

[15] http://euobserver.com/justice/119926 (accessed 7 July 2014).

in to obtain passenger data from all intra-EU flights (Council of the European Union, 2012: 2). The PNR data would then be collected by "Passenger Information Units" in the Member State of the origin or destination of the flight (Art. 4, 1) and be processed "against pre-determined criteria" (Art. 4, 2(a)), "against relevant databases, including international or national databases or national mirrors of Union databases" (Art. 4, 2(b)), "on a cases-by-case basis, to duly reasoned requests from competent authorities" (Art. 4, 2(c)), as well as "for the purpose of updating or creating new criteria for carrying out assessments" (Art. 4, 2(d)). The results of the processing would then be transferred to the defined competent authorities of the relevant Member States, and possibly on a case-by-case basis even to third countries (Art. 8). Data would be retained for a period of 30 days, but in an anonymized fashion for an additional five years, explicitly for purposes of the pro-active creation of new assessment criteria as defined in Art. 4, 2(d). This explicit scope highlights the significance of PNR data for new modes of data-driven profiling.

Theorizing profiling

Profiling is a powerful technique, and currently it experiences major changes that are related to the way in which knowledge about populations and futures is created. In post-9/11 security regimes, the efforts of policy makers to capture the future and fold it back into the present in order to render it actionable have reached new heights. The struggle with contingency and uncertainty in the 'war on terror' has been expressed in former US Secretary of Defence Donald Rumsfeld's statement about "unknown unknowns" in a speech at the NATO headquarters on 6 June 2002.[16] Dealing with the unpredictability of low-probability but high-impact events like terrorist attacks (Aradau and van Munster, 2007: 93), security agencies strive to get a grip of possible futures in order to mitigate the probabilities of the occurrence of events. The commodification of uncertainty as risk has been a key step of establishing such agency, even if there is no presumed calculability in the first place. As Beck (2002: 40) puts it: "As soon as we speak in terms of 'risk', we are talking about calculating the incalculable, colonizing the future." Such efforts to calculate what cannot be calculated have led to the notion of a risk society that makes use of anticipatory governance in order to "feign control over the uncontrollable" (Beck, 2002: 41). This pretense of real power over future contingencies, yet ontologically still grounded in the assumption that the world can be objectified, measured and calculated, has produced different modes of governing that considerably exceed the original notion of risk in an epistemological sense.

Ewald (2002) has retraced a genealogy of risk modes that proceeds from providence to prevention and eventually to precaution, and points out that the latter, in the vein of Rumsfeld's epistemological struggles, "bears witness to a deeply disturbed relationship with a science that is consulted less for the knowledge it offers that for the doubt it insinuates" (Ewald, 2002: 274). Precaution embraces contingency by moving beyond risk as a calculable objectification, however it appears still grounded in the assumption that the threat can somehow be known or experienced, even if it remains unclear what exactly it is and how it can be tackled. Such a notion of precaution stems from its origins in environmental protection (Aradau and van Munster, 2007; Beck, 2002). Anderson (2010a: 792) thus adds that precautionary measures seek to act before an identified threat reaches a point of irreversible damage, and such distinguishes precaution from preemptive measures. Preemption, as it

[16] http://www.nato.int/docu/speech/2002/s020606g.htm (accessed 7 July 2014).

embodies the logics of data-driven knowledge generation, ventures even further into the unknown, as it not merely acknowledges the fallibility of scientific knowledge, but strives to act "before the formation and identification of a determinate threat" (Anderson, 2010a: 792).

With the threat in the current EU security agenda being predominantly defined as terrorism and serious crime, traditional forms of profiling, so the reading I put forward here, enact a scientifically grounded mode of risk by running predefined terrorist/criminal profiles based on expert knowledge against the collected data. In the profile as such we can find no truth claim (in the form of scientific knowledge), but rather the establishment of possibility in the form of a hypothesis that builds on past experience. The underlying assumption here is that a passenger who embodies certain characteristics could turn out to become a threat, even if there is no objectified statement about the nature or likelihood of that threat. Profiling is thus enacted in a confirmatory or hypothesis-testing way to explore whether certain patterns of characteristics are represented in the analyzed population data, and if so, to put the identified individuals under scrutiny. In summary, the profile as the original *hypothesis* that provides grounds for further scrutiny is based on professional expertise. The new mode of data-driven profiling, on the other hand, so I argue, fully enacts a preemptive approach that decisively departs from expert knowledge and embraces the possibilities of large-scale analytics. As will be shown in more detail below, the construction of the profile subsequently differs considerably from what we find in traditional profiling practices. To be quite concise here: both modes construct hypotheses of suspicion on which security becomes enacted. The decisive difference between them, however, is that the former mode falls into the scope of the legal tools of the non-discrimination framework due to its static nature, while the latter manages to constantly escape the current regulatory regimes due to the fluidity of adaptive algorithms.

As a matter of fact, confirmatory profiling practices have raised considerable critique in terms of social sorting or racial profiling, as pre-defined profiles can include variables like gender, age, nationality, religious belief, etc. (Zarsky, 2011: 297). Tsoukala (2010: 44) points out that with confirmatory risk profiling "the target of social control shifts from the individual offenders to the members of deviant, 'risk-producing' groups, who are controlled on the ground of being suspects, at the present time, and potential offenders, in the future." In risk-based policing, it has been shown that certain societal subgroups have been identified as high-risk parts of the populations and have been repeatedly discriminated against, for instance North African youths in French suburbs, football supporters in the UK or Roma people in Italy (Tsoukala, 2010: 47-8). In terms of the 'war on terror', the debate on post-9/11 racial profiling against Muslims bears witness of such discriminatory practices (Harcourt, 2007; Harris and Schneier, 2012). Indeed, as Zedner (2006b: 426) adds, traditional profiling based on professional knowledge and long-term expertise is prone to oversimplification on the theoretical level. Profiles might be flawed with regard to apparent causalities or the neglect of conflicting variables. Thus, a majority of factors can contribute to the production of Type I errors and the high-risk flagging of innocent individuals whose personal data just by bad luck happens to represent what is believed to be the profile of a potential terrorist or criminal. As Pallitto and Heyman (2008: 321) point out, the reliance on risk in mobility tends to reinforce certain social categories like 'the other', 'the foreign' or 'the desperate', thus slowing down parts of the traveling population. On the other hand, "scrutiny directed at terror prevention (securitization) is often relaxed – when it threatens the movements of 'kinetic elites'" (Pallitto and Heyman, 2008: 326-7), thus connecting economic status to enhanced mobility. And while Adey emphasizes that mobility has always carried a strong notion of inequality, with airports

being genuine "difference machines" (Adey, 2008b), "dataveillance" (Amoore and de Goede, 2005) based on large amounts of passenger information arguably puts profiling and its consequences on a new structural level. In confirmatory profiling practices, the aforementioned caveats in the theoretical construction of profiles that are derived from professional knowledge and experience are prone to skew the analysis towards groups that become framed as more 'risky' than others, and thus potentially reinforce social imbalances. Subsequently, policy makers have been careful to implement anti-discriminatory safeguards into profiling regimes.

Profiling and non-discrimination

The principle of non-discrimination, also referred to as "principle of equality" or "non-discrimination clause" (Edel, 2010: 8-9), has been expressed as one of the cornerstones values of the European Union. It can be found throughout all major documents that lay the foundation of the normative framework of the EU and a broader geographical Europe, for instance in the Charter of Fundamental Rights of the European Union (European Union, 2000: Art. 21), the European Convention on Human Rights (European Court of Human Rights/Council of Europe, 2010: Art. 14/Art. 1 of Protocol No. 12) and the Treaty on the Functioning of the European Union (Art. 18-25). More specifically, the EU legal framework is composed of several Directives that implement the non-discriminatory treatment of persons, but focuses primarily on labor market issues (Gellert et al., 2013: 68). This rather fragmented field is set to be overcome by the pending Proposal for a Council Directive implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation (European Commission, 2008). Nonetheless, the non-discrimination framework that is applicable in the EU as of now lays down very specific regulations that ensure equal treatment of individuals within its jurisdiction. The PNR proposal itself refers to several of those safeguards, including the Charter of Fundamental Rights of the European Union, but also the proportionality principle and the EU Data Protection framework (95/46/EC). This scope on both non-discrimination and data protection does not come as a surprise, as "the issue at stake here is the discriminatory consequences of data processing operations" (Gellert et al., 2013: 63).

In order to prevent discrimination, as is being pointed out in the document, the construction of profiles from PNR data underlies ethical constraints, as "no such decision should discriminate on any grounds such as a person's sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation" (Council of the European Union, 2012: 8). While the effectiveness of such limitations in profiling can be challenged on the practical level, at least from a theoretical angle, a strong safeguard against discrimination and the reinforcement of social categories can be found here. Moreover, the proportionality principle establishes a purpose limitation for the analysis of PNR data, as "the processing of personal data must be proportionate to the specific security goals pursued by this Directive" (Council of the European Union, 2012: 7). The list of anti-discriminatory safeguards for profiling in the proposal is capped off by a reference to the EU Data Protection framework, stating that "every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress" (Art. 11, 1), thus providing a legal toolbox for the challenge of discriminatory issues on the individual level.

However, as will become apparent throughout the remainder of this paper, those safeguards only unfold their full regulatory power when applied to discrimination that arises from traditional practices of profiling that sort populations on the basis of pre-defined individual characteristics. Data-driven forms of profiling produce a distinct form of knowledge that appears dynamic and implicit, and thus continually escapes the scope of the regulatory legal regime. As a shift in the mode of data processing occurs, profiling might no longer be grasped by the direct and indirect anti-discriminatory approaches of the law. Or, put differently: what we are dealing with here appears to be a distinct, fluid mode of governing. Thus, how can we conceptualize new ways of knowledge construction and the ensuing consequences for security governance?

The 'new profiling' as data-driven governance

As has been pointed out above, profiling practices exceed the original logic of risk in epistemological terms, yet their governance rationale appears to be stuck in the ontological premise of an objectifiable world. Such a rift between knowledge creation and political practice and power, so the reading I put forward, can be best understood through a Foucauldian framework of governance. In fact, as Aradau and van Munster (2007: 101) claim, "a Foucauldian approach does not portray risks as calculable/incalculable, but rather focuses on 'how' presumably incalculable catastrophic risks like terrorism are governed", and thus can provide a better understanding of the shifts in profiling, and account for their implications for the governing of security. In his lectures at the Collège de France in 1976-79, Foucault (2003; 2007; 2008) has analyzed historical shifts of modes of power and governing. He claims that disciplinary power "breaks down individuals, places, time, movements, actions, and operations. It breaks them down into components such that they can be seen, on the one hand, and modified on the other" (Foucault, 2007: 56). It is essentially the practice that Haggerty and Ericson (2000) have later identified as the "surveillant assemblage" of a digitized era – the underlying mechanism of contemporary surveillance that disassembles individuals into "dividuals" (Deleuze, 1992) that consist of separate data points, in order to scrutinize, calculate, circulate and re-assemble them for distinct purposes. With regard to unfolding its normalizing power, discipline then proceeds by enforcing the disassembled individual to conform with a model of desired behavior and desired characteristics. As Foucault emphasizes, "it is not the normal and the abnormal that is fundamental and primary disciplinary power, it is the norm" (Foucault, 2007: 57). Norms can be considered the result of (informal) social negotiations, shaped by tradition and often codified in law. In the case of profiling, the applied norm that is determined to detect deviance is constructed *ex negativo* from what is desired. Such negative norms are profiling tools that are traditionally built on the "domain expertise" of security practitioners (McCue, 2007), using expert knowledge to define suspicious characteristics. In the PNR proposal, this practice is implemented in the presumed competences to "process PNR data against pre-determined criteria" (Art. 4, 2(a)). Thus, when a representation of the pre-defined profile is found in the database, the corresponding individual would be singled out from the passenger flow and further scrutinized. By setting up the suspicious profile as deviance from the norm, disciplinary power then ultimately forces the individual back into the norm in order not to pose a threat to society anymore.

However, in his analysis of contemporary security governance, Foucault proceeds beyond discipline and engages with the central question of how modern apparatuses of security differ from sovereignty and disciplinary power. Dealing with increasing mobility and the dissolution

of clear (national) boundaries of the exercise of power, the Foucauldian analysis thus turns to new ways of governing movement. In what has been deemed as the key step towards a "biopolitics of security" (Dillon and Lobo-Guerrero, 2008), Foucault suggests that instead of avoiding risks, security apparatuses embrace the concept of risk and profit from the emergence of (advanced) statistics, thus "finding support in the reality of the phenomenon, and instead of trying to prevent it, making other elements of reality function in relation to it, in such a way that the phenomenon is canceled out" (Foucault, 2007: 59). Starting from the population as the reference point, 'normality' is no longer defined by social or legal norms, but by the statistical normal distribution of characteristics. Such a turn then establishes "a plotting of the normal and the abnormal, of different curves of normality, and the operation of normalization consists in establishing an interplay between these different distributions of normality and in acting to bring the most unfavorable in line with the more favorable" (Foucault, 2007: 63). In terms of Anderson's analysis of anticipatory governance, such an embrace of analytics empowers new modes of risk – in this case from traditional to data-driven modes of profiling. Concerned with the detection of threats within the population, the latter empowers preemptive security measures that seek to act "over threats that have not yet emerged as determinate threats" (Anderson, 2010a: 790). Instead of applying old forms of knowledge in the form of professional expertise, data-driven profiling practices then produce a new form of knowledge that is not scientifically grounded and upholds no truth claims, but that derives directly from the analyzed population data.

Information and the ensuing intelligence have quickly become a major resource in security governance, as increasing availability of data as well as computational power now provide the possibilities to make sense of large amounts of (raw) data that had not been accessible before. In accordance with this trend, the eagerness to collect and combine data from mobile populations turns out to be a major theme in current EU efforts to fight terrorism and crime (Geyer, 2008). The creation of an European PNR system can be regarded as yet another stepping stone in the direction towards a proclaimed age of "Big Data" (Anderson, 2008; Manyika et al., 2011) in the security sector. Where traditional profiling meets its limits due to constraints in actual knowledge about terrorists and criminals, data-driven analytics go beyond the limits of the known and seek to unveil and rationalize the unknown. Not only do they seek to render the future actionable, they also promise to provide a glimpse at the future by creating a new and distinct form of knowledge about it.

Although Anderson (2010a: 790) rightly notes that such preemptive practices "break with the logic of risk […] as 'calculable uncertainty' based on the induction of frequency and harm from the past distribution of events", we can find a different form of 'riskiness' in data-driven profiling that comes into being via the analysis of statistical patterns. In fact we can find here close similarities to business models in the commercial sector. Consumer information that might seem irrelevant at the point of collection can now be turned into valuable knowledge later and in combination with other data. Put simply: the larger the database, the better the chances to detect patterns that reveal correlations between individual characteristics and consumer behavior – allowing for targeted advertising, custom-tailored services and individual offers. However, profiles that are produced and refined by algorithms do not only allow for personalization in the commercial sector, but also for preemptive practices in the security sector (Rouvroy, 2013). Data-driven analytics on a large-scale basis, as envisaged by a European PNR system, lift security practices to a new and seemingly limitless digital level that "involves the classification, compilation and analysis of data on, for example, passenger

information and financial transactions on an unprecedented scale" (Amoore and de Goede, 2005: 151).

The underlying rationale of such a new mode of making sense of the world culminates in the confidence to be able to predict security futures, as long as calculations are executed based on a sufficient amount of data (McCue, 2007). The mathematical 'law of large numbers' provides legitimacy for algorithmic findings in the data, which then in a second step become re-translated into interpretations of the real world in the form of *temporary* profiling hypotheses. As opposed to the commercial sector, the consequences of data-driven knowledges in security contexts can be rather serious. The identified profile still remains in the realm of negative evidence that necessarily has to be looked into, as it represents a (undefined) form of deviance. However, the re-assembly of the digitally encoded traveler might produce non-representational knowledge in terms of categories that do not reflect patterns of social reality (González Fuster et al., 2010: 2). In other words: the results could be rather arbitrary. The 'profile' then would remain an abstraction that could turn out to be a coincidental correlation as well as a spur of previously undetected causality. However, although data-driven profiles can merely serve to indicate conspicuousness, the detected 'suspicious' pattern in the security context must be scrutinized closer. And while the conspicuousness could possibly be unmasked as the aleatory correlation pattern that it is and the category would not stand in court, the instant consequences are material. As time constraints in security operations tend to put decision-making into the realm of urgency (McCue, 2007), ensuing actions become encoded in a dichotomous fashion – suspicion/non-suspicion results in scrutiny/no further scrutiny, and detention/free circulation. In this respect, traditional profiling and data-driven profiling do not so much differ in their consequences, as they both slow down mobility for the affected individuals assigned to the profile and can lead to intrusive secondary screening. However, as will be further shown, the two forms differ considerably in the mechanisms of how profiles come into being (expert knowledge vs. analytics) and in the targets they offer for safeguarding against discrimination (static vs. fluid).

The analysis of data-driven profiling requires us to rethink discrimination. As shown, the logics of discrimination in traditional profiling follow the establishment of a causal chain between indicators on the theoretical level and their representation in the population under scrutiny. By putting restraints on the choice of available variables for the construction of the theoretical foundations of profiles, undesired discrimination on the basis of certain characteristics such as sex, race or religion, possibly might be canceled out. However, with data-driven analytics, this is not the case. While still starting from the notion of the individual as an information source, the collective level of the profile becomes more prone to the production of arbitrary categories instead of real communities. As such categories come into being via probabilistic assumptions, de Vries (2010: 81) notes that the individual is likely to be left puzzled, wondering "what do *I* have to do with the 199 hypothetically similar people who are terrorists? [emph. in orig.]"

Large-scale analytics, or the "crunching of numbers" (Ayres, 2007), proclaim the triumph of rationalization over biased and flawed human interaction. A human operator can deliberately or involuntarily discriminate, but a machine is free from such bias. Its truth lies in the seemingly objective algorithmic calculations and the results it produces based on the available data. It is a different form of knowledge about the world that is being produced here, though, a new form of truth regime that Rouvroy (2013) calls "data behaviourism", seeking to eradicate the unknown parts of the contingency equation. In terms of Beck's (2002) "risk

society", algorithmic interpretations of the world do no longer attempt to *feign* control over the future, but seek to *obtain* control by applying rational calculations, and thus strive to gain access to a reality that has been measured and framed in numeric terms. Analyzing the impact of such a digital encoding of the reality, Hansen and Porter (2012: 417) note that numbers can indeed "complement and displace linguistically articulated norms." Equally as important for the understanding of the effects of data-driven profiling is that numbers can be updated and replaced quickly and constantly. With the constant production of data in digitized everyday interactions, the information stored in databases possesses a rather dynamic character. As a consequence, data-driven profiles are no longer static categories but a fluid phenomenon, coming into being as "spontaneous germinations" (Rouvroy, 2013: 146).

For instance, profiling algorithms based on Bayesian systems can handle and process "continuous streams of transaction-generated information to routinely update and adjust the system's assessments of risk" (Gandy, 2010: 29). As opposed to deterministic types of algorithms that produce the same result over and over when run against the same database and which are likely to struggle in complex environments (Anrig et al., 2008: 79), such learning systems require a certain level of training through cross-validation by a human operator. However, once a Bayesian network is set up, updates in the database can be analyzed and incorporated automatically. This fluidity signifies a major change in the conceptualization of profiling, as it creates only momentary groupings that might be disappearing back into the white noise of the database in the next moment. Often referred to as neural networks due to their similarities to the human brain, such systems can pose considerable hurdles in terms of the interpretation of results. As their internal processes remain opaque and "the information 'learned' from the data is somewhat hidden in the network and cannot be used as evidence for the result" (Anrig et al., 2008: 78), the outputs of data-driven analytics are presented in simplified numeric terms or graphical representations, or they even remain completely removed from the realm of human readability. However, what has been deemed as the overcoming of human irrationality, circumventing interpretation as a source of error and discrimination (Zarsky, 2011), then essentially puts data-driven profiling into a black box. Categories then come into being as part of autonomic machine behavior, processed and communicated between systems that do not require human intervention (Hildebrandt, 2008).

Thus, data-driven profiling creates a rather separate technique of governing that differs considerably from traditional, expertise-based ways of profiling. As outlined, distinct modes of anticipation result in distinct accounts of the world. Knowledge as the reference category for sorting flows of global mobility can either rely on actual experiences from the past or on the analysis of the population as the subject to be governed in the present. As suggested, the different modes of profiling fall well into the Foucauldian analysis of power that conceptualizes a series of governmental types that proceeds from sovereignty to discipline and then ultimately to security (Collier, 2009). The typology of profiling introduced here should not be mistaken as a clear-cut analytical scheme, though. On the contrary, it appears more appropriate to interpret the distinction between traditional and data-driven profiling as the construction of Weberian ideal types. The artificial super-elevation of disciplinary vs biopolitical modes of governing is not likely to stand in empirical analyses of security regimes that seldom feature clear-cut, but rather overlapping modes of governing. As Foucault himself clarifies, "there is not the legal age, the disciplinary age, and then the age of security. Mechanisms of security do not replace disciplinary mechanisms, which would have replaced juridico-legal mechanisms" (Foucault, 2007: 8). Such a conceptualization of overlapping modes can clearly be found in the PNR proposal, as it seeks to deploy traditional "real-time"

(Art. 4, 1(a)) and data-driven "pro-active" (Art. 4, 1(d)) types of profiling in a parallel fashion, and moreover combining them with checks against remote databases and individual in-depth scrutiny. As Collier (2009: 79) emphasizes, the scope should thus lie on a "'topological' analysis of power that examines how existing techniques and technologies of power are re-deployed and recombined in diverse assemblies of biopolitical government." An analysis of how profiling practices enact power over mobile populations in the name of the 'war on terror' subsequently must not stop at defining distinct governing formations, but has to proceed further and look into how patterns of correlation among different forms of power assemble contemporary apparatuses of security (Collier, 2009: 89). Understanding the Foucauldian framework as a problematization of spaces of government, the mode of governing such an assemblage becomes clearer when "tracing the recombinatorial processes through which techniques and technologies are reworked and redeployed (Collier, 2009: 93). The remaining part of this paper thus engages with the topology created by the relationships between traditional and data-driven types of profiling and the ensuing consequences for the non-discrimination framework.

Out of sight, out of mind?

Arguably, the findings so far present major challenges for anti-discriminatory safeguards. First of all, with the data-driven creation of 'suspicious' profiles, we can find a loss of traceability. Increasing amounts of data and computational power have enabled security practices in which "data mining techniques remain a technological black box for citizens" (Hildebrandt and Gutwirth, 2008: 367). With only machine readable outputs of neural networks, it becomes increasingly hard to understand, let alone challenge categories that result from data-driven forms of profiling. Second, and maybe more important, we can find a loss of visibility. Contemporary practices of collecting and processing of data tend to blend into an environment of ubiquitous computing or "Ambient Intelligence" (de Vries, 2010) that interacts with the individual on an automated and invisible basis, thus enabling practices of profiling to increasingly operate out of sight. As data-driven profiles produce artificial and non-representational categories rather than actual real-life social groups, the individual is likely to not even notify when they become part of a 'risky' category. Gandy (2010: 39) thus emphasizes that "most of the time, persons who have been victimized by a routine system error will not know precisely if, when, or how they have been discriminated against." Only that in the case of data-driven profiling, the occurrence of discrimination will not be based on a system error but on the functional logic of correlative pattern discovery. Moreover, it can be assumed that a large percentage of the data used for profiling is collected by the private sector originally for business purposes (González Fuster et al., 2010: 4) and that security measures are merely a form of secondary use. PNR data had been collected by airlines long before security agencies were drawn to this additional data source in the aftermath of 9/11. However, in large-scale analytics, there can by definition be no such thing as 'secondary use', as every bit of information could become valuable in the future without revealing its utility in the present. Only as analytics unveil what is hidden in databases can the purpose of data collection be defined *a posterio*. Here we find a serious conflict with the European data protection framework. Neither the proportionality principle nor purpose limitations can apply to the reversed logics of data-driven profiling, as both start from the assumption that the goals of data collection and processing are clear in advance of the actual procedure.

Third and finally, from the losses of traceability and visibility results a loss of accountability. The PNR proposal clearly states that no decision shall be based exclusively on the basis of PNR data, but that further investigation must undergo human review (Council of the European Union, 2012: 16). However, this is a deceptive safeguard, as data-driven profiling in security screening relies on the assumptions that all revealed patterns must necessarily be scrutinized in order to find out whether they pose an actual threat. But as the output of neural networks is most likely only machine readable, the human operator must act on the basis of the translation of algorithmic terms into risk levels. Thus, the real-life consequences for the affected individual that falls into the generated category do not vanish, nor do they become mitigated by human review. On the contrary, the human reviewer themselves loses true agency, as they only enact what algorithmic categorizations indicate. What we are facing in the case of inductive knowledge generation is not 'assistance' in decision making, but rather a prescription of human reviewer conduct. As Matzner (2013) points out, cognitive systems that are supposed to assist human operators (such as airport security systems with visual alerts) are based on informational accounts of the world that are inaccessible for humans (i.e., large-scale analytics), and thus require a certain level of 'trust' in the applied algorithmic calculations. This results in what Brey (2005: 392) calls "semi-autonomous information-processing systems", in which the human operator, though entitled to an autonomous decision, is rendered likely to comply to the truth claims of the algorithm. After all, such an epistemological gap appears to be "intrinsic to the expected functionality and benefits of using cognitive systems as assistance to human operators" (Matzner, 2013). In a crafty move, public authorities thus take away their own agency when it comes to the level of security measures that is to be applied to the members of a risk category. But as agency is re-located into the realm of dynamic realm of learning algorithms, neither the engineer nor the operator can understand or even explain why someone has been singled out for secondary screening. As Introna (2013) puts it, "design decisions, encoded and encapsulated in complex nests of logical and control statements […] enact (in millions of lines of source code) our supposed choices based on complex relational conditions, which after many iterations of 'bug fixing' and 'tweaking' *even the programmers no longer understand* [emph. in orig.]" Consequently, affected individuals effectively lose their ability to challenge decisions, as the accountability for the creation of the profile is hidden in algorithmic processes and the population of travelers.

Data-driven governance and non-discrimination

Thus, assuming that apparatuses of security always possess a strategic notion (Dillon, 2010: 63), what can we learn from the re-assembly of profiling elements on the political level? Or, put differently: what are the governing practices of data-driven profiling? Deploying professional expertise as well as generating new knowledge for the sake of the paradigm of free movement of the 'good' parts of the population, the role of the law within this assemblage appears to be crucial as it diminishes due to the non-applicability of its tools. We encounter a tension between the law and 'normality', as normality does no longer derive from a static norm but is constantly re-configured. As normality transforms into a dynamic "mobile norm" (Amoore, 2011), deviance from that norm becomes equally dynamic. Security subsequently becomes governed through mobile profiles that serve as *temporary hypotheses* of risk. Those hypotheses are not up for contest, but rather must be re-connected to the real world in order to cancel out the possibilistic mode of threat that is created by the algorithm.

As has been shown, what we can find here is a deep-seated epistemological conflict between an anti-discrimination framework that conceives of knowledge as the establishment of causality, and data-driven analytics that build fluid hypotheses on the basis of correlation patterns in dynamic databases. This rift eventually causes a diminishing effectiveness of the anti-discrimination toolbox.

There are a number of conceptual consequences from the outlined developments. It has been argued that in contemporary security regimes, the individual is not the central category of interest anymore, but that categories are the new way to cope with ever-increasing complexity and large-scale databases (Rouvroy, 2013). Thus, there is a lingering question whether 'profiling' is still the right terminology for data-driven modes of knowledge generation, after all. As traditional profiles are being replaced by non-representative categories, the disciplinary obligation to adapt individual characteristics and behavior to pre-defined norms also vanishes. Hildebrandt and Gutwirth (2008: 368) note that "citizens are faced with profiling practices that make it possible to control and steer individuals without a need to identify them", as individuals blur into the liquidity of constantly updated databases. This raises the further question whether the "dream of targeted governance" (Valverde and Mopas, 2004) has to be reconsidered. What matters in the assessment of risk is the category, not the individual that falls in and out of that category. After all, the preemptive category itself might only be momentary, collapsing back into the informational stream as databases are constantly updated and thus change the population and possible patterns of correlation that can be found therein. As Gillespie (2014) points out, "algorithms are made and remade in every instance of their use because every click, every query, changes the tool incrementally."

Generally speaking, we might be witnessing a further disappearance of governing from the public realm, where it can be challenged and critiqued (Rouvroy, 2013). In security governance, the future must necessarily be rendered actionable by folding it back into the present, but the technique of folding is undergoing change as its tools are re-assembled and re-combined. New forms of algorithmic risk assessment remove the mechanisms of security governance from the eye, leaving behind a new series of hyper-rationalized discrimination issues (Gandy, 2010) that pose major hurdles for the legal tools of traditional anti-discriminatory safeguards. When measured against the claims of a "Europe built on fundamental rights" as expressed in the Stockholm Programme, policy tools such as the pending EU PNR Directive present a serious challenge for the ethical principle of non-discrimination by fostering new and data-driven forms of profiling. As is noted in the Stockholm Programme, "basic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established" (European Council, 2010: C 115/19). However, as has been shown, it appears highly questionable whether these safeguards can still be effective after the arrival of large-scale analytics in the realm of security.

Conclusions

This paper has aimed at critically engaging discriminatory pitfalls that emerge from the application of data-driven analytics that produce temporary 'profile hypotheses' for the purpose of governing mobile populations. It is not exactly a new insight that "profiling through predictive data mining is already a reality worldwide, including the European Union" (González

Fuster et al., 2010: 1). However, the increasing amount of security practices that rely on algorithmic analyses of large-scale databases poses a rather bleak outlook. In the EU, systems such as SIS I + II, VIS and an European PNR system have been rendered as cornerstones for providing European law enforcement agencies with the tools of fighting terrorism and crime through new forms of future-related governance. Such data-driven security practices do not only imply practical consequences, but relate to the theoretical framing of changing security regimes as well. This paper has connected Foucauldian thought of governing to emerging technologies and their implementation on the political level in order to outline conceptual consequences for the specific case of profiling and its impact on the non-discrimination framework. Despite a rather theoretical scope, an effort has been made to connect the findings with empirical evidence from the EU security policy-making process. Using the European PNR proposal as an example for the assembly of distinct but nonetheless related and overlapping modes of profiling, it has been shown how changing types of knowledge generation unfold a distinct mode of governing that re-assembles the relation between normality, deviance, and the applicability of legal tools. From the perspective of a topological analysis, the role of juridical elements thus seems to diminish behind the opacity of black boxes, within which learning algorithms remove the dichotomous categorization of suspicion/non-suspicion from the visible and legally governable realm of debate, challenge and critique. A Foucauldian lens enables us to retrace how through data-driven profiling practices, we are witnessing a reconfiguration of normality and deviance in the context of security, empowering suspicion to become mobile and ever-adaptive.

PNR data is easily collected at all stages of a journey, covering a temporal and spatial range from booking and payment up to special dietary requirements during the flight. Ensuing risk-based security governance through profiling practices that becomes enacted on the basis of hidden data collection is in itself rather liquid and creates the profile/category only for the moment of scrutiny. It becomes visible just for a short period in which a high-risk assessment, derived from data-driven analytics, triggers real-life consequences that slow down mobility and set off potentially invasive secondary screening. Aviation is but one, although maybe the most striking example for the use data-driven profiling based on information about mobile populations. However, with the envisaged interoperability of European security systems and databases, it is likely that new forms of knowledge generations will be found on broader levels. Thus, can the non-discrimination framework and data-driven profiling be reconciled such that legal tools can regain their effectiveness?

With regard to the challenges of black-boxed risk assessment (and also with regard to how such practices transform concepts of privacy), Hildebrandt and Gutwirth (2008: 367) call for transparency enhancing tools in order to re-open the black boxes of algorithms and shed light on the mechanisms of how profiles and categories come into being. However, such an approach could turn out to be difficult. As Introna (2013) puts it, “the algorithm is a black box, which when opened simply introduces more black boxes, which when subsequently opened simply introduces more black boxes, and so forth.” Since questions concerning how exactly profiles are brought into being are seldom answered by public authorities (González Fuster et al., 2010: 8), reverse engineering could provide another opportunity to re-open the black box. Such an effort must consist of “articulating the specifications of a system through a rigorous examination drawing on domain knowledge, observation, and deduction to unearth a model of how that system works” (Diakopoulos, 2013). However, due to the dynamic nature of algorithms, reverse engineering can provide only momentary snapshots of data-driven profiling practices that might not be relevant any longer at the point of discovery. As Gillespie

(2014) little optimistically states, “there may be something, in the end, impenetrable about algorithms.” If not for an indeed improbable uncovering of the realm of algorithms, further research then must engage with in-depth empirical analyses of how distinct modes of governing in security regimes become re-assembled and re-combined in order to advance our understanding about the creation of security knowledge. As Foucault (2003: 242) notes, we should in fact conceive of a biopolitics of security that “does not exclude disciplinary technology, but it does dovetail into it, integrate it, modify it to some extent, and above all, use it by sort of infiltrating it, embedding itself in existing disciplinary techniques”, therefore accounting for further empirical dynamics.

IV. Conclusions

"We went back stage; we learned about the skills of practitioners; we saw innovations come into being; we felt how risky it was; and we witnessed the puzzling merger of human activities and non-human entities."
(Latour, 2005: 90)

The 'so what?' question

The 'assorted inquiries in aviation' offered in this thesis have, at least this much I hope, provided some small insights into the many ways security unfolds. They have targeted a number of practices, social relations, and political agendas. They have looked into normative questions of justice, accountability, and responsibility. They have highlighted multiple political, social, and economic rationalities. And they have shown how the initially postulated paradox of security emerges and re-emerges as a defining paradigm of our everyday lives. Each one of them offers some very specific conclusions for the empirics studied, and at times even some more general thoughts. But the one thing they have not yet provided, and which is arguably the final missing piece in this thesis, is a *connected conclusion* on the theoretical level. Implications for how to think about security, that is. The narratives have not yet answered the one question that Thomas Diez, during my years as a PhD student, has put forward as often as painstakingly and precisely: 'so what?' The 'so what?' question probes academic work on multiple levels and could be re-framed in a number of slightly different ways: What is the relevance of my research? Does it provide added value? Where does this lead to? Can I create any political or social impact with my work? What would such impact look like? This list could be continued. In fact, I do think that in a research field as sensitive as security studies, such questions need to be asked and dealt with. Thus, in the last and concluding narrative, I seek to address the 'so what?' question by taking up on the first nine narratives and coming up with an approximation to a conclusion for security. Paraphrasing the title of this very project: what has this analysis of security been *on*? Is there a common frame that could serve as an outcome of this all? I remain reluctant to propose a definite answer – too fragmented, too dispersed, and too wide-ranging are the notions of security in both theoretical and empirical terms. However, I would like to propose a reading of security that appears suitable across all areas and that moreover highlights the need for a moral stance: security as *normativity*.

Last narrative: security as normativity

The last narrative closes the bracket. We have started out by exploring the value of security as a basic principle of social and political life, before diving into the manifold stories about how the impossibility of security plays out among various registers of ontology and epistemology, of politics and the economy, and not least of the social. In whatever way security becomes embedded into technologies, into questions of governing, and extends itself into the future, we must always keep in mind that security remains some sort of auxiliary construct for the sake of something else – be it 'the good life', epistemological closure in terms of (feigned) foresight, or just more money in the bank. Security might not have a specific agenda (Bigo and Tsoukala, 2008b: 4), but despite the multiple facets it is used in, it retains a normative core – however one that is all too often overshadowed by its political instrumentalization. As Huysmans (2008: 178) puts it, "politics becomes fragmented and dispersed within the societal", and this last narrative reaches out to re-capture such fragmentation and dispersion of security politics and re-fold them into a framework of normativity. Whereas the first nine narratives have been carved out in a rather descriptive fashion (with the occasional hint to the normative dimension, admittedly), this last narrative is *prescriptive*.

The notion of security as normativity must not be misunderstood as an ontological quest. The question here is not 'What should security look like?' – public discourse has all too often been

reduced to such a simplistic yet borderless formula. The question should rather be: 'How can we think and research security such that its value core persists and its detrimental potentials might be canceled out to the fullest extent possible?' Put differently: how can security escape its own pathology? Again, we must keep in mind here that security, security politicalities and security socialities need by no means be congruent. This has become apparent by the empirics provided and their takes on the dispersed assemblage of actors, rationalities, and practices that constitute airport security. However, besides their thematic scope that targets the broad field of aviation, the analytical inquiries of this thesis are unified by a thread of normativity. They all take up on the 'so what?' question in one form or another. What do we make from academic analysis? Especially when considering the "normative dilemma of writing security" (Huysmans, 2002), critical security studies must never remain on a descriptive level, however abstract it might be. On the contrary, and this is where we have to return to the initial narrative of security as value, academia has to advance one step further and engage the normative consequences of security (and insecurity). As Browning and McDonald (2013: 250) claim, "if there is a consistency across critical security studies scholarship in this sense, it is that ethical commitments are evident (in commitments to resistance, desecuritization or emancipation, for example) but are insufficiently developed to provide a genuine account of what constitutes ethical action regarding security." How to enact such ethical commitments, and how to provide a modest attempt to develop them, then?

If, as Der Derian (1995: 26) claims, "a late modern security [is] comfortable with a plurality of centers, multiple meanings, and fluid identities", then an agenda of critical security studies must aim at unsettling those centers, at challenging those meanings, and at questioning those identities it produces. The tools for this have been laid out. As Salter (2008d: 30) notes, "critical theory questions the evolution of current systems in terms of the interests, actors and possible fields of action. In particular, critical theorists have challenged the labeling of particular issues as security issues by political or corporate elites and the attendant policy choices." In order to establish the possibility for an ethics of security in the first place, we must then carefully unpack assemblages of security – we must understand how they have come about, we must understand how they amplify or mute certain actors and interests, and we must understand which governmental rationalities underpin them. Security studies must not refrain from such complexity. On the contrary, as Rose (1999: 276) claims, "to analyse, then, is not to seek for a hidden unity behind this complex diversity", but to embrace messiness and expose it to moral judgment.

As has been pointed out throughout both theoretical and empirical accounts in this thesis, security practices and discourses can indeed be 'bad'. Any critical agenda of thinking about security in fact prescribes probing the very question whether security plays out good or bad. As the c.a.s.e. collective (2006: 456) argues, "uncovering the realities of security (or rather insecurity) entails locating human rights abuses, the oppression of minorities, the powerlessness of the poor and violence against women." In this vein, Burgess (2009: 319) adds that security practices and discourses "have important ethical implications, the most consequential among which is the risk of discriminating, through information processing, entire categories of population." Thus, moral judgment appears vital to any critical stance towards security as both a means of critique and an agenda-setting tool for some kind of 'better' security.

As we have seen, not only is security burdened with normative issues, but also is the more general notion of government. As Dean (2006: 11) frames it, "if morality is understood as the

attempt to make oneself accountable for one's own actions, or as a practice in which human beings take their own conduct to be subject to self-regulation, then government is an intensely moral activity." In this sense, ordering the social through the register of security presents a double challenge for normativity. Critique must be directed at the governing through security, as well as at security itself. This is not to suggest that security techniques, security practices, security technologies, or security discourses would present themselves as detachable from rationalities of government. Rather, security unfolds through more than one domain. Subsequently, any critical security studies agenda must open up to all possible registers of security – some of which have been touched upon in the narratives told in section I. of this thesis. In short: we must create an account of both rationalities and means of security. As Neocleous (2008: 5) radically puts it, we must "challenge the ways in which security has become the master narrative through which the state shapes our lives and imaginations (security risks here, security measures there, security police everywhere), producing and organising subjects in a way that is always already predisposed towards the exercise of violence in defence of the established order." How can we do this?

In order to answer this question as completely as possible, we must first turn to another, auxiliary question: which avenues of critique does security as normativity open up? Arguably, one can take multiple routes here. The first route would be to derive *resistance* from the notion of normativity. In order to empower such a normative imperative of resisting security, it becomes then necessary to first disassemble security such that it can be rendered visible and intelligible. The ensuing task must then be "to disturb and destabilize these regimes, to identify some of the weak points and lines of fracture in our present where thought might insert itself in order to make a difference" (Rose, 1999: 277), and critical academia is primed to do just that. Resistance challenges power. And more so, it challenges the distinct discourses and practices of security that have sought to establish such power in the first place. But it can only do so on an informed basis. We must then strive to provide an understanding of how security is shaped and re-shaped, how it is constantly transformed and applied according to governmental rationalities and political programs. As Huysmans (2008: 178) summarizes such a scholarly agenda of resistance: "in analyzing how power operates through dispersed, fragmented practices that nevertheless weave a diagram of constituting and governing societal relations, the total categories in which politics has been conceptualized in the constitutional framing of exception-state versus society, law versus politics, sovereignty-collapse into a relational picture of various expert discourses, professional knowledges, institutional practices governing a biological and economic understanding of life, and a rich history of sociopolitical struggles."

A second route of security as normativity can be directly derived from such analyses. If, as has been shown throughout this thesis, a major trajectory of critique towards security consists of its often opaque and black-boxed character, both in terms of its emergence and of its functioning, then we must think about how to re-open security. Once its configurations have been rendered visible, it can be brought into the public arena and exposed to the fundamental principles of *democracy*. As Bigo (2012: 278) explains, "democratizing security supposes then to examine how these professionals deliver their different truth(s) about the danger in the world, and to put them in context." Security as normativity must then challenge the narratives of security as technology, as economy, and as securitization through the lens suggested by the Paris school. It must look into the entangled multi-national networks of professionals of security, into security discourses that build on domain expertise, and at the intersections between those networks and the security industry. Building on that, it must also closely

scrutinize technologies. As de Goede (2011: 16) rightfully points out, "assembly with private spaces and technologies strengthens actual security practices, while rendering them less accountable", thus calling for careful analysis of technologies. If, as Huysmans (1998: 249) argues, "in security studies the ethico-political dimensions are often buried under a technical logic of necessity", such a logic must be rendered questionable by prying it away from the realm of practical expertise and exposing it to the normative principles of the realm of human rights. As Huysmans (1998: 249) rightfully adds, indeed "the question 'What happens when we do this?' slips out the interpretation" all too often.

A third route for security as normativity once again derives from the former one. If security can be re-captured and folded into the scope of democratic principles, then it can in fact become *emancipatory*. Security as normativity in this vein must challenge marginalizations and exclusions that come into being through security in the first place. As Bigo (2012: 278) puts forward such a claim, "the voices of the 'undesirables', that [have been] excluded through security-based social sorting, need to be heard and sometimes listened to in order to change notions of danger, security, and normal activity, as a form of freedom." While Bigo makes a powerful claim here, it might be argued that critical thought must not stop at those who suffer from security, but must also consider the multiple forces, stakes, and interests that have been marginalized along the way of shaping security in the first place. In such fashion, we must think again about the narrative of security as government and the ensuing narrative of security as assemblage. If security must be conceptualized as "controversy" (Schouten, 2014a) or "ambiguity" (de Lint and Virta, 2004), then what about the voices that have been muted in its constitution? And what does that tell us about the voices that *have* been heard? As Rose (1999: 279) compellingly frames the problematic: "something might be learnt from those insurgent, minority or subaltern forces that have often refused to codify themselves, that have resisted the temptations of party and programme, that have taken shape in the shadows, interstices and oversights of conventional politics and that have so often acted as laboratories for alternative futures." Ultimately, if we pursue the potential for emancipation further, we must even ask if the challenge of normativity might not lead us to emancipation *from* security, as has been put forward by Neocleous (2008), for instance. Such a stance then re-connects to the narrative of security as securitization. As Huysmans (1998: 234) argues, calling for the re-establishment of 'normal politics', "one has to decide not only how important security is but also if one wants to approach a problem in security terms or not."

Politics that are not framed in terms of security are normal politics. Securitization theory has intensely dealt with the rift between normality and exception, even up to the point where Taureck (2006: 57) distinguishes between "securitization the theory" and "securitization the normative practice" – the former dealing with matters of the exception and the latter dealing with attempts of re-establishing normality. If indeed, as the c.a.s.e. collective (2007: 571) claims, "the question as to how a political order that is constituted through a securitized limit can be resisted, challenged or unmade", then such a challenge must necessarily work through the limit itself. The limit is all too often the reference point for a politics of security that appears to have forgotten how life can be conceived of as not constantly on the brink. As has been shown, the pathology of security is its inevitable reversal effect on our ontological state. Thinking and speaking about security always implies danger, uncertainty, and threat that is already on its way. Security as normativity, however, needs to opt for *normality*. If, as Dillon (2011: 780) claims, "security discourses specify the politics of peace in terms of the unfolding of burgeoning discourses of danger and spiraling security problematizations, threatening fields of formation, surfaces of friction, adversarial relations, irreconcilable enmities, and war

in the name of life itself", then we must challenge such discourses. Security as normativity must unsettle the foundations on which those discourses are built.

Normal politics, as opposed to the exceptional logics of threat, would then also require a different take on the future. A take that is not dominated by the permanent anticipation of the 'event' on all levels, thus empowering the full spectrum of security measures in order to intervene into the future or at least mitigate its effects through the layer of ultimate preparedness – even if such a bleak future has not, and might never, materialize. A fifth route for security as normativity would then be to challenge the *logics of futurity* that enact such a key role in discourses of security. This might well be the hardest quest there is for critical security studies. As has been shown throughout the narrative of security as future, both contingency and its political transformation are limitless. If probability is not enough, simply opt for possibility. If you cannot statistically extrapolate the event, then just imagine it. And if by doing that you might merely feign control over what by any logics can never be controlled? Maybe that is not the main point, and maybe it never has been. If, as has been laid out, security is a means of ordering the social, then its government must be legitimized through political modulations of the future. That is, through the canceling out of any conceivable threats. However, as the horizon of threats has been expanded beyond the limits of knowledge, there remains no border to what security must not do. As de Goede (2011: 17) summarizes this conflict, "precautionary security and proportionality are *always* in tension with each other [emph. in orig.]." Security as normativity would then have to challenge the politics of speculation and of possibilities in order to expose their epistemologically unfounded excess. This is not to say that security might not be about the future anymore. A security politics that is not about the future ceases to be a politics in the first place. However, a normatively more responsible security politics must refrain from circular logics of virtual, yet not necessarily materializing threats that empower a spiral of always new and ever more excessive security measures (Massumi, 2007).

What might be a suitable mode to do so? We might need to be willing to acknowledge the fact that security is indeed always on the brink – simply because life itself is always on the brink. The contingency of life is what brought us here in the first place. As Rose (1999: 24) lays out, "the discovery of new problems for government – and the invention of new forms of government – embraces, recodes, reshapes those that pre-exist them", and thus enables security politics through the constant discovery, construction, and transformation of new threats. If we are stuck in such circular logic, then is it indeed necessary what the c.a.s.e. collective (2007: 574) has suggested: to empower security as normativity by "exploring in which ways the political can be imagined against, beyond or outside of security"? Do we in fact need to aim for a security politics *beyond security*? Such a notion certainly seems tempting, especially if considering the manifold detrimental effects that security can unfold across all registers of the social. However, it would also to some extent neglect the complications of security as government and security as assemblage, and re-introduce the notion of an overarching security agenda that can somehow be overcome. Moreover, the call for a security politics beyond security would not necessarily resolve the issue, after all. If one governmental agenda would be re-placed by another, would that not rather shift than solve the problem? By claiming the need to go beyond security, we would claim the power and authority that we seek to challenge in the first place. Security as normativity clearly presupposes criticality – but, as Buzan and Hansen (2010: 660) argue, "one problem is that we have no yardstick for what is a 'truly' critical – or critical enough – account" of security.

Figuring out what is critical, after all, has been deemed a major stake for critical security studies. As the c.a.s.e collective (2006: 476) argues, "we need to ask ourselves, as researchers […], what the claim of being 'critical' […] entails for our engagement with the political." However criticality might eventually be conceived of, analyzing politics indeed brings about close proximity to politics, and such opens up possible ways to actively intervene into the politicality of security. Thus, a viable route for security as normativity appears to be the engagement with politics. Security, as has been argued, can effectively be challenged by scrutinizing and exposing the processes of its emergence. However, this is only the first step. Security as normativity, if taken seriously, entails a complete *re-politicization* of security. That is to pry security away from the realm of emergency and to "bring back social and political issues to the realm of the political" (c.a.s.e. collective, 2006: 476) through very concrete engagements with very concrete politics. After all, "being critical means adhering to a rigorous form of sceptical questioning, rather than being suspicious or distrustful in the vernacular sense of those terms" (c.a.s.e. collective, 2006: 476), and questioning is an integral part of any democratic politics. Political programs must necessarily undergo scrutiny and questioning, most notably through parliamentary debates and the media, before they can be molded into concrete legislation. Here we find one of the cracks in the processes of government that opens up space for critical thought and intervention.

One has to be very careful about the modes of doing so, however. Particularly, the c.a.s.e. collective has dealt in depth with the consequences of political intervention from academia. As they argue, "engaging with bureaucracies and the professionals of politics is a 'two-way-track'" (c.a.s.e. collective, 2007: 564) that inevitably turns the researcher into an accountable actor themselves. Here, we must keep in mind the slippery slope of possibly contributing to processes of securitization through an engagement, however critical it might be, with discourses of security, thereby potentially reinforcing them involuntarily. Any attempt to actively intervene into the political shaping of security also brings about a second series of pitfalls. Can we, as academics, indeed claim to speak truth to power, and thus claim authority over how security should be concretely crafted? To think critically, as the c.a.s.e. collective (2006: 476) reminds us, "is also to recognize oneself as being partially framed by those regimes of truth, concepts, theories and ways of thinking that enable the critique." If we take seriously the Foucauldian claim that power is relational and always emergent, then academic agency is not excluded from this. If we as scholars are willing to grasp such power, then we must be prepared for the accountability that comes with it. Security as normativity clearly must intervene, but it must be careful not to fall into the same political traps that it challenges.

In fact, there are many routes to engage security as normativity (and certainly more than I have sketched out here). All of them are neither easy nor comfortable. On the contrary, they require us to step out of the ivory tower of academia and occupy a clearly defined societal position. Critiquing security can quickly turn oneself from a scholar into a target. Entering politics can be exhausting, dull, and frustrating. Nonetheless, security clearly appears to be worth the fight. If, as has been outlined here, we conceive of security as a powerful technique of government, then we might even be obligated to critically engage with the conduct of our own conduct. As Rose (1999: 41) painfully reminds us, to think about government is to think about ourselves and our role within assemblages of security: "are we to be governed as members of a flock to be led, as children to be coddled and educated, as a human resource to be exploited, as members of a population to be managed, as legal subjects with rights, as responsible citizens of an interdependent society, as autonomous individuals with our own illimitable aspirations, as value-driven members of a moral community"? Different

rationalizations of security request us to enact different roles. However, it remains within our own autonomy and agency to challenge those assigned roles.

Conceiving security as normativity subsequently also means to conceive government as ethical obligation. As Rose (1999: 284) has it, “to the extent that we are governed in our own name, we have a right to contest the evils that are done to us in the name of government, a right that we acquire from our birth and life at the point of convergence of practices of government themselves.” As has been shown throughout this thesis, and running the risk of sounding redundant by now, there are multiple concrete ‘evils’ that come into being in the name of security every single day. More often than not, however, they remain hidden in entangled networks, in obscure practices, in remote databases, or in proprietary algorithms. In this vein, academia must not shy away from the task of analytically uncovering the multiple natures of security that we find empirically, and subsequently making them accessible to the public level. My modest hope is that the inquiries presented here can in some way provide a small contribution to this task. Security as normativity prescribes “to disrupt depoliticizing practices and discourses of security in the name of exceptionality, urgency or bureaucratic expertise, and bring them back to political discussions and struggles” (c.a.s.e. collective, 2006: 476) – in short: to the principles of democracy. In this vein, an analysis of government through security, as Dean (2006: 37-8) puts forward, “enhances human capacity for the reflective practice of liberty, and the acts of self-determination this makes possible, without prescribing how that liberty should be exercised.” A truly ethical task it is then, indeed.

References

9/11 Commission (2004) Final Report of the National Commission on Terrorist Attacks Upon the United States. Available at: http://govinfo.library.unt.edu/911/report/911Report.pdf (accessed 7 July 2014). Washington, D.C.: National Commission on Terrorist Attacks.

Abeyratne R (2010) Full Body Scanners at Airports—The Balance Between Privacy and State Responsibility. *Journal of Transportation Security* 3(2): 73-85.

Accenture (2007) Facilitation of Aviation Security: Feasability Study of "Registered Passenger" Concept. Final Report. Brussels: European Commission Directorate-General Energy & Transport.

ACI/AEA (2011) Joint Briefing Aviation Security: 10 Years on from 9/11. Available at: http://files.aea.be/News/Joint_ACI_AEA.pdf (accessed 7 July 2014).

Acuto M and Curtis S (2014) Assemblage Thinking in International Relations. In Acuto M & Curtis S (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations.* Basingstoke/New York: Palgrave Macmillan, 1-16.

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

Adey P (2004b) Surveillance at the Airport: Surveilling Mobility/Mobilising Surveillance. *Environment and Planning A* 36(8): 1365-1380.

Adey P (2006) "Divided we Move": The Dromologics of Airport Security and Surveillance. In Monahan T (ed.) *Surveillance and Security. Technological Politics and Power in Everyday Life.* New York/London: Routledge, 195-208.

Adey P (2008a) Airports, Mobility and the Calculative Architecture of Affective Control. *Geoforum* 39(1): 438-451.

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

Adey P (2009) Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body. *Environment and Planning D: Society and Space* 27(2): 274-295.

Adey P (2010) *Aerial Life: Space, Mobilities, Affects.* Malden/Oxford/Chichester: Wiley-Blackwell.

Adey P and Anderson B (2012) Anticipating Emergencies: Technologies of Preparedness and the Matter of Security. *Security Dialogue* 43(2): 99-117.

Adey P, Bissell D, McCormack D and Merriman P (2012) Profiling the Passenger: Mobilities, Identities, Embodiments. *Cultural Geographies* 19(2): 169-193.

Agamben G (2005) *State of Exception.* Chicago/London: University of Chicago Press.

Aggarwal C C (2007) On Randomization, Public Information and the Curse of Dimensionality. Paper presented at IEEE 23rd International Conference on Data Engineering, Istanbul, 11-15 April. Available at: http://charuaggarwal.net/curse.pdf (accessed 7 July 2014).

Aggarwal C C and Yu P S (2005) On Variable Constraints in Privacy Preserving Data Mining. Paper presented at SIAM International Conference on Data Mining, Newport Beach, 21-23 April. Available at: http://charuaggarwal.net/aggar140.pdf (accessed 7 July 2014).

Aggarwal C C and Yu P S (eds.) 2008. *Privacy-Preserving Data Mining: Models and Algorithms,* New York: Springer Science+Business Media.

Altman I (1977) Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues* 33(3): 66-84.

Ammicht Quinn R (2014) Sicherheitsethik: Eine Einführung. In Ammicht Quinn R (ed.) *Sicherheitsethik.* Wiesbaden: Springer VS, 15-47.

Amoore L (2006) Biometric Borders: Governing Mobilities in the War on Terror. *Political Geography* 25(3): 336-351.

Amoore L (2009) Algorithmic War: Everyday Geographies of the War on Terror. *Antipode* 41(1): 49-69.

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

Amoore L (2013) *The Politics of Possibility: Risk and Security Beyond Probability.* Durham/London: Duke University Press.

Amoore L and de Goede M (2005) Governance, Risk and Dataveillance in the War on Terror. *Crime, Law and Social Change* 43(2): 149-173.

Amoore L and de Goede M (2008a) Introduction: Governing by Risk in the War on Terror. In Amoore L & de Goede M (eds.) *Risk and the War on Terror.* London/New York: Routledge, 5-20.

Amoore L and de Goede M (eds.) 2008b. *Risk and the War on Terror,* London/New York: Routledge.

Amoore L and Hall A (2009) Taking People Apart: Digitized Dissection and the Body at the Border. *Environment and Planning D: Society and Space* 27(3): 444-464.

Amoore L and Hall A (2013) The Clown at the Gates of the Camp: Sovereignty, Resistance and the Figure of the Fool. *Security Dialogue* 44(2): 93-110.

Anderson B (2010a) Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies. *Progress in Human Geography* 34(6): 777-798.

Anderson B (2010b) Security and the Future: Anticipating the Event of Terror. *Geoforum* 41(2): 227-235.

Anderson B and Adey P (2012) Governing Events and Life: 'Emergency' in UK Civil Contingencies. *Political Geography* 31(1): 24-33.

Anderson C (2008) The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *Wired* (16.07).

Anrig B, Browne W and Gasson M (2008) The Role of Algorithms in Profiling. In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 65-88.

Aradau C (2010) Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 41(5): 491-514.

Aradau C, Lobo-Guerrero L and Van Munster R (2008) Security, Technologies of Risk, and the Political: Guest Editors' Introduction. *Security Dialogue* 39(2-3): 147-154.

Aradau C and van Munster R (2007) Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations* 13(1): 89-115.

Augé M (2006) *Non-places: Introduction to an Anthropology of Supermodernity.* London: Verso.

Ayres I (2007) *Super Crunchers: Why Thinking-by-Numbers is the New Way to be Smart.* New York: Bantam Books.

Bærenholdt J O (2013) Governmobility: The Powers of Mobility. *Mobilities* 8(1): 20-34.

Ball K and Webster F (2003) The Intensification of Surveillance. In Ball K & Webster F (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age.* London/Sterling: Pluto Press, 1-15.

Balzacq T (2010) Constructivism and Securitization Studies. In Dunn Cavelty M & Mauer V (eds.) *The Routledge Handbook of Security Studies.* Milton Park/New York: Routledge, 56-72.

Balzacq T (2011) A Theory of Securitization: Origins, Core Assumptions, and Variants. In Balzacq T (ed.) *Securitization Theory: How Security Problems Emerge and Dissolve.* London/New York: Routledge, 1-30.

Balzacq T, Basaran T, Bigo D, Guittet E-P and Olsson C (2010) Security Practices. In Denemark R A (ed.) *International Studies Encyclopedia Online. Available at: http://www.blackwellreference.com/public/tocnode?id=g9781444336597_chunk_g978144433659718_ss1-2 (accessed 7 July 2014).* Blackwell.

Barnett A (2004) CAPPS II: The Foundation of Aviation Security? *Risk Analysis* 24(4): 909-916.

Barros X (2012) EU Counterterrorism and Aviation Security: Supranational Rules but Intergovernmental Politics? *European Foreign Affairs Review* 17(2/1): 53-69.

Bayley D and Shearing C (1996) The Future of Policing. *Law and Society Review* 30(3): 585-606.

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

Beck U (1999) *World Risk Society.* Cambridge: Polity Press.

Beck U (2002) The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society* 19(4): 39-55.

Bellanova R and Duez D (2012) A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage. *European Foreign Affairs Review* 17(2/1): 109–124.

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

Bennett C J (2005) What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11. In Zureik E & Salter M B (eds.) *Global Surveillance and Policing. Borders, Security, Identity.* Cullompton/Portland: Willan, 113-138.

Bennett C J (2008) Unsafe at Any Altitude: The Comparative Politics of No-Fly Lists in the United States and Canada. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 51-76.

Bennett C J (2011) In Defence of Privacy: The Concept and the Regime. *Surveillance & Society* 8(4): 485-496.

Bennett C J, Raab C D and Regan P M (2003) People and Place: Patterns of Individual Identification within Intelligent Transportation Systems. In Lyon D (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London/New York: Routledge, 153-175.

Bentham J (1995) Panopticon. In Božovič M (ed.) *The Panopticon Writings.* London: Verso, 29-95.

Bergson H (1911) *Laughter: an Essay on the Meaning of the Comic.* New York: Macmillan.

Biersteker T J (2010) Interrelationships Between Theory and Practice in International Security Studies. *Security Dialogue* 41(6): 599-606.

Bigo D (1994) The European Internal Security Field: Stakes and Rivalries in a Newly Developing Area of Police Intervention. In Anderson M & den Boer M (eds.) *Policing Across National Boundaries.* London/New York: Pinter, 161-173.

Bigo D (2001) The Möbius Ribbon of Internal and External Security(ies). In Albert M, Jacobson D & Lapid Y (eds.) *Identities, Borders, Orders: Rethinking International Relations Theory.* Minneapolis/London: University of Minnesota Press, 91-116.

Bigo D (2002) Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political* 27(1): 63-92.

Bigo D (2008a) Globalized (in)security. The Field and the Ban-opticon. In Bigo D & Tsoukala A (eds.) *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes after 9/11.* London/New York: Routledge, 10-48.

Bigo D (2008b) Security: A Field Left Fallow. In Dillon M & Neal A W (eds.) *Foucault on Politics, Security and War.* Basingstoke/New York: Palgrave Macmillan, 93-114.

Bigo D (2012) Security, Surveillance and Democracy. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 277-284.

Bigo D, Bonelli L, Chi D and Olsson C (2007) Mapping the Field of the EU Internal Security Agencies. In Bigo D (ed.) *The Field of the EU Internal Security Agencies.* Paris: L'Harmattan, 5-66.

Bigo D and Jeandesboz J (2010) The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5. Available at: http://www.ceps.eu/system/files/book/2010/02/INEX%20PB5%20e-version.pdf (accessed 7 July 2014).

Bigo D and Tsoukala A (eds.) 2008a. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11,* London/New York: Routledge.

Bigo D and Tsoukala A (2008b) Understanding (in)security. In Bigo D & Tsoukala A (eds.) *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11.* London/New York: Routledge, 1-9.

Bigo D and Walker R B J (2007) Political Sociology and the Problem of the International. *Millennium - Journal of International Studies* 35(3): 725-739.

Bissell D, Hynes M and Sharpe S (2012) Unveiling Seductions Beyond Societies of Control: Affect, Security, and Humour in Spaces of Aeromobility. *Environment and Planning D: Society and Space* 30(4): 694-710.

BMBF (2007) Research for Civil Security. Review: Fields of Research and Contacts. Available at: http://www.bmbf.de/pub/forschung_fuer_zivile_sicherheit_eine_bestandsaufnahme.pdf (accessed 7 July 2014).

BMBF (2012) Research for Civil Security 2012 - 2017. Framework Program: High tech Strategy. Available at: http://www.bmbf.de/pub/rahmenprogramm_sicherheitsforschung_2012.pdf (accessed 7 July 2014).

BMI (2010) Press Release: Body Scanner Trial Run at Hamburg Airport, 27 September 2010.

BMI (2011) Press Release: Body Scanner Trial Run: Efficient, but not applicable nationwide, 31 August 2011.

Bonß W and Wagner K (2012) Risiken und symbolische Politik: Anmerkungen zu einem Konzept und seiner Bedeutung für die Luftsicherheit. In Gerhold L & Schiller J (eds.) *Perspektiven der Sicherheitsforschung. Beiträge aus dem Forschungsforum Öffentliche Sicherheit.* Frankfurt am Main/Berlin/Bern/Bruxelles/New York/Oxford/Wien: Peter Lang, 41-55.

Booth K (1991) Security and Emancipation. *Review of International Studies* 17(4): 313-326.

Booth K (2005a) Critical Explorations. In Booth K (ed.) *Critical Security Studies and World Politics.* Boulder/London: Lynne Rienner Publishers, 1-20.

Booth K (ed.) 2005b. *Critical Security Studies and World Politics,* Boulder/London: Lynne Rienner Publishers.

Boyle P and Haggerty K D (2012) Planning for the Worst: Risk, Uncertainty and the Olympic Games. *The British Journal of Sociology* 63(2): 241-259.

Brey P (2005) The Epistemology and Ontology of Human-Computer Interaction. *Minds and Machines* 15(3/4): 383-398.

Browning C S and McDonald M (2013) The Future of Critical Security Studies: Ethics and the Politics of Security. *European Journal of International Relations* 19(2): 235-255.

Brownsword R (2008) Knowing Me, Knowing You - Profiling, Privacy and the Public Interest. In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 345-364.

Büger C (2014) Thinking Assemblages Methodologically: Some Rules of Thumb. In Acuto M & Curtis S (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations.* Basingstoke/New York: Palgrave Macmillan, 58-66.

Burgess J P (2009) There is No European Security, Only European Securities. *Cooperation and Conflict* 44(3): 309-328.

Burgess J P (2011) Ethical Review and the Value(s) of Security Research. *Paper presented at the Workshop Ethical Issues in Security Research – a Practical Approach, Brussels, 29 September.*

Burgess J P (2012) The Societal Impact of Security Research, PRIO Policy Brief 09/2012. Available at: http://file.prio.no/Publication_files/Prio/Burgess-Societal-Impact-Policy-Brief-9-2012.pdf (accessed 7 July 2014).

Buzan B and Hansen L (2009) *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Buzan B and Hansen L (2010) Beyond The Evolution of International Security Studies? *Security Dialogue* 41(6): 659-667.

Buzan B, Wæver O and de Wilde J (1998) *Security: A New Framework for Analysis.* Boulder: Rienner.

c.a.s.e. collective (2006) Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue* 37(4): 443-487.

c.a.s.e. collective (2007) Europe, Knowledge, Politics — Engaging with the Limits: The c.a.s.e. collective Responds. *Security Dialogue* 38(4): 559-576.

Cavoukian A (2009a) Privacy by Design. Available at: http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (accessed 7 July 2014).

Cavoukian A (2009b) Whole Body Imaging in Airport Scanners: Building in Privacy by Design. Available at: http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf (accessed 7 July 2014).

Cavoukian A, Taylor S and Abrams M E (2010) Privacy by Design: Essential for Organizational Accountability and Strong Business Practices. *Identity in the Information Society* 3(2): 405-413.

Cavusoglu H, Byungwan K and Raghunathan S (2010) An Analysis of the Impact of Passenger Profiling for Transportation Security. *Operations Research* 58(5): 1287-1302.

Cheney-Lippold J (2011) A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society* 28(6): 164-181.

Clarke R (2009) Privacy Impact Assessment: Its Origins and Development. *Computer Law & Security Review* 25(2): 123-135.

Coates J (2007) Talk in a Play Frame: More on Laughter and Intimacy. *Journal of Pragmatics* 39(1): 29-49.

Collier S J (2009) Topologies of Power: Foucault's Analysis of Political Government beyond 'Governmentality'. *Theory, Culture & Society* 26(6): 78-108.

Connolly W E (2013) The 'New Materialism' and the Fragility of Things. *Millennium - Journal of International Studies* 41(3): 399-412.

Coser R L (1959) Some Social Functions of Laughter: A Study of Humor in a Hospital Setting. *Human Relations* 12(2): 171-182.

Council of the European Union (2012) 8916/12. Proposal for a Directive of the Council and the European Parliament on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, 23 April 2012. Brussels: Council of the European Union.

Curry M R (2004) The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation. *Surveillance & Society* 1(4): 475-499.

Custer B, Calders T, Schermer B and Zarsky T (eds.) 2013. *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases,* Heidelberg/New York/Dordrecht/London: Springer.

Daase C and Kessler O (2007) Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger. *Security Dialogue* 38(4): 411-434.

Davis M S (1995) The Sociology of Humor: A Stillborn Field? *Sociological Forum* 10(2): 327-339.

de Goede M (2005) Carnival of Money: Politics of Dissent in an Era of Globalizing Finance. In Amoore L (ed.) *The Global Resistance Reader.* London/New York: Routledge, 379-391.

de Goede M (2008a) Beyond Risk: Premediation and the Post-9/11 Security Imagination. *Security Dialogue* 39(2-3): 155-176.

de Goede M (2008b) Money, Media and the Anti-politics of Terrorist Finance. *European Journal of Cultural Studies* 11(3): 289-310.

de Goede M (2011) European Security Culture. Preemption and Precaution in European Security. Inaugural Lecture, 27 May 2011. Amsterdam: University of Amsterdam.

de Goede M and Randalls S (2009) Precaution, Preemption: Arts and Technologies of the Actionable Future. *Environment and Planning D: Society and Space* 27(5): 859-878.

de Hert P and Bellanova R (2011) *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals.* Washington, DC: Migration Policy Institute.

de Lint W and Virta S (2004) Security in Ambiguity: Towards a Radical Security Politics. *Theoretical Criminology* 8(4): 465-489.

de Pauw E, Ponsaers P, van der Vijver K, Bruggeman W and Deelman P (eds.) 2011. *Technology-led Policing,* Antwerpen/Apeldoorn/Portland: Maklu.

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

Dean M (2006) *Governmentality: Power and Rule in Modern Society.* London/Thousand Oaks/New Delhi: Sage Publications.

Deleuze G (1992) Postscript on the Societies of Control. *October* 59: 3-7.

Deleuze G and Guattari F (1987) *A Thousand Plateaus: Capitalism and Schizophrenia.* Minneapolis: University of Minnesota Press.

Der Derian J (1995) The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard. In Lipschutz R D (ed.) *On Security.* New York/Chichester: Columbia University Press, 24-45.

Diakopoulos N (2013) Rage Against the Algorithms. The Atlantic, 3 October. Available at: http://www.theatlantic.com/technology/archive/2013/10/rage-against-the-algorithms/280255/ (accessed 7 July 2014).

Dillon M (2010) Biopolitics of Security. In Burgess J P (ed.) *The Routledge Handbook of New Security Studies.* Milton Park/New York: Routledge, 61-71.

Dillon M (2011) Specters of Biopolitics: Finitude, *Eschaton*, and *Katechon*. *South Atlantic Quarterly* 110(3): 780-792.

Dillon M and Lobo-Guerrero L (2008) Biopolitics of Security in the 21st Century: An Introduction. *Review of International Studies* 34(2): 265-292.

Dupont B (2006) Power Struggles in the Field of Security: Implications for Democratic Transformation. In Wood J & Dupont B (eds.) *Democracy, Society and the Governance of Security.* Cambridge: Cambridge Univ. Press, 86-110.

ECORYS (2009) Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies - ENTR/06/054: Final Report. Brussels: ECORYS Research and Consulting.

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

Edgerton D (2007) *The Shock of the Old. Technology and Global History Since 1900.* Oxford/New York: Oxford University Press.

Elias B (2010) *Airport and Aviation Security. U.S. Policy and Strategy in the Age of Global Terrorism.* Boca Raton/London/New York: CRC Press.

Elmer G (2012) Panopticon-Discipline-Control. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 21-29.

Epstein C (2007) Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders. *International Political Sociology* 1(2): 149-164.

Ericson R V (1994) The Division of Expert Knowledge in Policing and Security. *British Journal of Sociology* 45(2): 149-175.

Ericson R V (2006) Ten Uncertainties of Risk-Management Approaches to Security. *Canadian Journal of Criminology and Criminal Justice* 48(3): 345-357.

Ericson R V and Haggerty K D (1997) *Policing the Risk Society.* Oxford: Clarendon Press.

Eriksson J and Rhinard M (2009) The Internal-External Security Nexus: Notes on an Emerging Research Agenda. *Cooperation and Conflict* 44(3): 243-267.

European Commission (2004) COM(2004) 74 final. On the Implementation of the Preparatory Action on the Enhancement of the European Industrial Potential in the Field of Security Research: Towards a Programme to Advance European Security Through Research and Technology. Brussels.

European Commission (2008) COM(2008) 426 final. Proposal for a Council Directive on Implementing the Principle of Equal Treatment Between Persons Irrespective of Religion or Belief, Disability, Age or Sexual Orientation. 2 July. Brussels.

European Commission (2010a) COM(2010) 311 final. On the Use of Security Scanners at EU Airports. 15 June. Brussels.

European Commission (2010b) COM(2010) 2020 final. Europe 2020: A strategy for Smart, Sustainable and Inclusive Growth. 3 March. Brussels.

European Commission (2011a) COM(2011) 808 final. Horizon 2020 - The Framework Programme for Research and Innovation. 30 November. Brussels.

European Commission (2011b) COM(2011) 810 final. Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules for the Participation and Dissemination in 'Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)'. 30 November. Brussels.

European Commission (2011c) High Level Conference "Protecting Civil Aviation Against Terrorism", Brussels, 27 September 2011, Conclusions and Recommendations. Available at: http://ec.europa.eu/transport/modes/air/events/doc/2011-09-27-avsec-conclusions.pdf (accessed 7 July 2014).

European Commission (2011d) SEC(2011) 1427 final. Commission Staff Working Paper: Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 - The Framework Programme for Research and Innovation'. 30 November. Brussels.

European Commission (2012a) COM(2012) 417 final. Action Plan for an Innovative and Competitive Security Industry. 26 July. Brussels.

European Commission (2012b) Ethical and Regulatory Challenges to Science and Research Policy at the Global Level. Brussels: Directorate-General for Research and Innovation.

European Commission (2012c) EU Security Research: Safeguarding Society, Boosting Growth. Luxembourg: Publications Office of the European Union.

European Commission (2012d) FP7-SEC-2013-1 Call Fiche. 10 July. Brussels.

European Commission (2012e) SWD 143 final. Commission Staff Working Document on Transport Security. 31 May. Brussels.

European Council (2010) 2010/C 115/01. The Stockholm Programme - An Open and Secure Europe Serving and Protecting Citizens. 4 May. Brussels: Official Journal of the European Union.

European Court of Human Rights/Council of Europe (2010) European Convention on Human Rights.

European Parliament (2011) A7-0216/2011. Report on Aviation Security, with a Special Focus on Security Scanners. Committee on Transport and Tourism. Rapporteur: Luis de Grandes Pascual. 30 May. Strasbourg.

European Security Research & Innovation Forum (2009) ESRIF Final Report. Available at: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (accessed 7 July 2014).

European Security Research Advisory Board (2006) Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board. Luxembourg: Office for Official Publications of the European Communities.

European Security: High Level Study on Threats Responses and Relevant Technologies (2006) Deliverable D6-1 (Final Report): New European Approaches to Counter Terrorism, 21 March.

European Union (2000) Charter of Fundamental Rights of the European Union. *2000/C 364/01, 18 December.*

European Union (2010) Internal Security Strategy for the European Union: Towards a European Security Model. Luxembourg: Publications Office of the European Union.

Ewald F (2002) The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution. In Baker T & Simon J (eds.) *Embracing Risk: The Changing Culture of Insurance and Responsibility.* Chicago/London: The University of Chicago Press, 273-301.

Feeley M M and Simon J (1992) The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology* 30(4): 452-474.

Fine G A and de Soucey M (2005) Joking Cultures: Humor Themes as Social Regulation in Group Life. *Humor - International Journal of Humor Research* 18(1): 1-22.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Foucault M (1980) The Confession of the Flesh. In Gordon C (ed.) *Power/Knowledge: Selected Interviews and Other Writings 1972-1977.* New York: Vintage Books, 194-228.

Foucault M (1984a) On the Genealogy of Ethics: An Overview of Work in Progress. In Rabinow P (ed.) *The Foucault Reader.* New York: Pantheon Books, 340-372.

Foucault M (1984b) Right of Death and Power Over Life. In Rabinow P (ed.) *The Foucault Reader.* New York: Pantheon Books, 258-272.

Foucault M (1994) *The Birth of the Clinic: An Archaeology of Medical Perception.* New York: Vintage Books.

Foucault M (2003) *Society Must Be Defended. Lectures at the Collège de France, 1975-76.* London: Penguin Books.

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

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

Frederickson H G and LaPorte T R (2002) Airport Security, High Reliability, and the Problem of Rationality. *Public Administration Review* 62(1): 33-43.

Friedewald M, Wright D, Gutwirth S and Mordini E (2010) Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework. *Innovation: The European Journal of Social Science Research* 23(1): 61-67.

Frimpong A (2011) Introduction of Full Body Image Scanners at the Airports: A Delicate Balance of Protecting Privacy and Ensuring National Security. *Journal of Transportation Security* 4(3): 221-229.

Fuller G and Harley R (2004) *Aviopolis. A Book about Airports.* London: Black Dog.

Gamble A (1995) The New Political Economy. *Political Studies* 43(3): 516-530.

Gandy O H (1993) *The Panoptic Sort: A Political Economy of Personal Information.* Boulder: Westview.

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

Gellert R, de Vries K, de Hert P and Gutwirth S (2013) A Comparative Analysis of Anti-Discrimination and Data Protection Legislations. In Custer B, Calders T, Schermer B & Zarsky T (eds.) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases.* Heidelberg/New York/Dordrecht/London: Springer, 61-89.

Geyer F (2008) Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice. Challenge Research Paper No. 9 Available at: http://www.libertysecurity.org/IMG/pdf_Databases_and_Systems_of_Information_Exchange_in_the_Area_of_Freedom_Security_and_Justice.pdf (accessed 7 July 2014).

Giemulla E M and Rothe B R (2008) *Recht der Luftsicherheit.* Berlin/Heidelberg: Springer.

Gillespie T (2014) The Relevance of Algorithms. In Gillespie T, Boczkowski P & Foot K (eds.) *Media Technologies: Essays on Communication, Materiality, and Society.* Cambridge: MIT Press, 167-194.

Gilliom J (2011) A Response to Bennett's 'In Defence of Privacy'. *Surveillance & Society* 8(4): 500-504.

Goffman E (1974) *Frame Analysis: An Essay in the Organization of Experience.* Boston: Northeastern University Press.

González Fuster G, Gutwirth S and Ellyne E (2010) Profiling in the European Union: A high-risk Practice. INEX Policy Brief 10 / June 2010. Available at: http://www.ceps.eu/system/files/book/2010/06/INEX%20PB10%20Fuster%20et%20al.%20on%20Profiling%20in%20the%20EU%20e-version.pdf (accessed 7 July 2014). PRIO.

Group of Personalities in the Field of Security Research (2004) Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research. Luxembourg: Office for Official Publications of the European Communities.

Grusin R (2010) *Premediation: Affect and Mediality After 9/11.* New York: Palgrave Macmillan.

Guild E and Carrera S (2010) The European Union's Area of Freedom, Security and Justice Ten Years On. In Guild E, Carrera S & Eggenschwiler A (eds.) *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme.* Brussels: Centre for European Policy Studies, 1-12.

Guillaume X (2014) *Agencement* and Traces: A Politics of Ephemeral Theorizing. In Acuto M & Curtis S (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations.* Basingstoke/New York: Palgrave Macmillan, 106-112.

Guittet E-P and Jeandesboz J (2010) Security Technologies. In Burgess J P (ed.) *The Routledge Handbook of New Security Studies.* Milton Park/New York: Routledge, 229-239.

Guzzini S (2011) Securitization as a Causal Mechanism. *Security Dialogue* 42(4-5): 329-341.

Haggerty K D (2004) Ethics Creep: Governing Social Science Research in the Name of Ethics. *Qualitative Sociology* 27(4): 391-414.

Haggerty K D and Ericson R V (2000) The Surveillant Assemblage. *British Journal of Sociology* 51(4): 605-622.

Hainmüller J and Lemnitzer J M (2003) Why do Europeans Fly Safer? The Politics of Airport Security in Europe and the US. *Terrorism and Political Violence* 15(4): 1-36.

Hansen H K and Porter T (2012) What Do Numbers Do in Transnational Governance? *International Political Sociology* 6(4): 409-426.

Hansen L (2008) From Camps to Conversations in Critical Security Studies. *International Studies Review* 10(3): 652-654.

Harcourt B E (2007) Muslim Profiles Post-9/11: Is Racial Profiling an Effective Counter-terrorist Measure and Does It Violate the Right to be Free from Discrimination? In Goold B J & Lazarus L (eds.) *Security and Human Rights.* Oxford/Portland: Hart Publishing, 73-98.

Harrington J E (2014) Dear America, I Saw You Naked - And Yes, We Were Laughing. Confessions of an ex-TSA Agent. 30 January, available at www.politico.com/magazine/story/2014/01/tsa-screener-confession-102912.html (accessed 7 July 2014).

Harris S and Schneier B (2012) To Profile or Not to Profile? A Debate between Sam Harris and Bruce Schneier, 25 May, available at http://www.samharris.org/blog/item/to-profile-or-not-to-profile (accessed 7 July 2014).

Harrison J (2009) *International Aviation and Terrorism. Evolving threats, evolving security.* London/New York: Routledge.

Harvey D (2005) *A Brief History of Neoliberalism.* Oxford/New York: Oxford University Press.

Hayes B (2006) *Arming Big Brother: The EU's Security Research Programme.* Amsterdam: Transnational Institute/Statewatch.

Hayes B (2009) *NeoConOpticon. The EU Security-Industrial Complex.* Amsterdam: Transnational Institute/Statewatch.

Hayes B (2010) "Full Spectrum Dominance" as European Union Security Policy: on the Trail of the "NeoConOpticon". In Haggerty K D & Samatas M (eds.) *Surveillance and Democracy.* Milton Park/New York: Routledge, 148-170.

Hayes B (2012) The Surveillance-Industrial Complex. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 167-175.

Heath-Kelly C (2012) Can We Laugh Yet? Reading Post-9/11 Counterterrorism Policy as Magical Realism and Opening a Third-Space of Resistance. *European Journal on Criminal Policy and Research* 18(4): 343-360.

HIDE and RISE Projects (2010) Whole Body Imaging at Airport Checkpoints: The Ethical and Policy Context. Policy Report 2010/01, http://www.cssc.eu/public/ETHICS-OF-BODY-SCANNER-POLICY-REPORT.pdf (accessed 7 July 2014).

Hildebrandt M (2008) Defining Profiling: A New Type of Knowledge? In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 17-46.

Hildebrandt M and Gutwirth S (2008) Concise Conclusions: Citizens out of Control. In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 365-368.

Hildebrandt M, Verfaillie K and van Brakel R (undated) SIAM Deliverable 4.2: Literature Overview of Freedom Infringements.

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

Huysmans J (1998) Security! What Do You Mean? From Concept to Thick Signifier. *European Journal of International Relations* 4(2): 226-255.

Huysmans J (2002) Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security. *Alternatives: Global, Local, Political* 27(1): 41-62.

Huysmans J (2006) *The Politics of Insecurity. Fear, Migration and Asylum in the EU.* Milton Park/New York: Routledge.

Huysmans J (2008) The Jargon of Exception - On Schmitt, Agamben and the Absence of Political Society. *International Political Sociology* 2(2): 165-183.

Huysmans J (2011) What's in an Act? On Security Speech Acts and Little Security Nothings. *Security Dialogue* 42(4-5): 371-383.

IATA (2011) Checkpoint of the Future Executive Summary.Available at: https://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf (accessed 7 July 2014).

ICAO (2012) Communiqué of the ICAO High Level Conference on Aviation Security, Montréal, 12 to 14 November 2012. Available at: http://www.icao.int/Meetings/avsecconf/Documents/HLCAS%20-%20Communique%2014%20September%202012.pdf (accessed 7 July 2014).

Introna L D (2013) Algorithms, Performativity and Governability. *Governing Algorithms: A Conference on Computation, Automation, and Control, 16-17 May.* New York University.

Jackson B, Chan E and LaTourrette T (2012) Assessing the Security Benefits of a Trusted Traveler Program in the Presence of Attempted Attacker Exploitation and Compromise. *Journal of Transportation Security* 5(1): 1-34.

Jacobson S H (2012) Watching through the "I"s of Aviation Security. *Journal of Transportation Security* 5(1): 35-38.

Jenkins R (2012) Identity, Surveillance and Modernity: Sorting Out Who's Who. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 159-166.

Johnston L and Shearing C D (2003) *Governing Security: Explorations in Policing and Justice.* London/New York: Routledge.

Jones R (2009) Checkpoint Security. Gateways, Airports and the Architecture of Security. In Aas K F, Gundhus H O & Lomell H M (eds.) *Technologies of InSecurity. The Surveillance of Everyday Life.* London: Routledge-Cavendish, 81-102.

Jones T and Newburn T (1996) The Regulation and Control of the Private Security Industry. In Saulsbury W, Mott J & Newburn T (eds.) *Themes in Contemporary Policing.* London: Policy Studies Institute.

Jones T and Newburn T (2002) The Transformation of Policing? Understanding Current Trends in Policing Systems. *British Journal of Criminology* 42(1): 129-146.

Kaunert C and Léonard S (2012) Introduction: Supranational Governance and European Union Security after the Lisbon Treaty - Exogenous Shocks, Policy Entrepreneurs and 11 September 2001. *Cooperation and Conflict* 47(4): 417-432.

Klauser F R, Ruegg J and November V (2008) Airport Surveillance between Public and Private Interests: CCTV at Geneva International Airport. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 105-126.

Klein N (2007) *The Shock Doctrine: The Rise of Disaster Capitalism.* London: Penguin Books.

Kroener I and Neyland D (2012) New Technologies, Security and Surveillance. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 141-148.

Kuipers G (2008) The Sociology of Humor. In Raskin V (ed.) *The Primer of Humor Research.* Berlin/New York: Mouton de Gruyter, 365-402.

Kuipers G (2011) The Politics of Humour in the Public Sphere: Cartoons, Power and Modernity in the First Transnational Humour Scandal. *European Journal of Cultural Studies* 14(1): 63-80.

Lahav G (2008) Mobility and Border Security: The U.S. Aviation System, the State, and the Rise of Public-Private Partnerships. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 77-104.

Lakoff A (2006) Techniques of Preparedness. In Monahan T (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life.* New York/London: Routledge, 265-274.

Latour B (2005) *Reassembling the Social: an Introduction to Actor-Network-Theory.* Oxford: Oxford Univ. Press.

Leese M (2013) Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs. *Computer Law & Security Review* 29(5): 480-490.

Lippert R and O'Connor D (2003) Security Assemblages: Airport Security, Flexible Work, and Liberal Governance. *Alternatives: Global, Local, Political* 28(3): 331-358.

Lipschutz R D (1995) On Security. In Lipschutz R D (ed.) *On Security.* New York/Chichester: Columbia University Press, 1-23.

Lisle D (2014) Energizing the International. In Acuto M & Curtis S (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations.* Basingstoke/New York: Palgrave Macmillan, 67-74.

Lloyd J (2003) Airport Technology, Travel, and Consumption. *Space and Culture* 6(2): 93-109.

Loader I (1997) Thinking Normatively About Private Security. *Journal of Law and Society* 24(3): 377-394.

Loader I (1999) Consumer Culture and the Commodification of Policing and Security. *Sociology* 33(2): 373-392.

Loader I and Walker N (2001) Policing as a Public Good: Reconstituting the Connections Between Policing and the State. *Theoretical Criminology* 5(1): 9-35.

Loader I and Walker N (2004) State of Denial? Rethinking the Governance of Security. *Punishment & Society* 6(2): 221-228.

Loader I and Walker N (2006) Necessary Virtues: the Legitimate Place of the State in the Production of Security. In Wood J & Dupont B (eds.) *Democracy, Society and the Governance of Security.* Cambridge: Cambridge Univ. Press, 165-195.

Lobo-Guerrero L (2011) *Insuring Security. Biopolitics, Security and Risk.* Milton Park/New York: Routledge.

LuftSiG (2005) German Aviation Security Act, 11 January 2005.

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

Lyon D (2003b) Introduction. In Lyon D (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London/New York: Routledge, 1-10.

Lyon D (2003c) Surveillance after September 11, 2001. In Ball K & Webster F (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age.* London/Sterling: Pluto Press, 16-25.

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

Lyon D (2006a) Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9/11 in Context. *Canadian Journal of Criminology and Criminal Justice* 48(3): 397-411.

Lyon D (ed.) 2006b. *Theorizing Surveillance. The Panopticon and Beyond,* Cullompton/Portland: Willan.

Lyon D (2006c) Why Where You Are Matters: Mundane Mobilities, Transparent Technologies, and Digital Discrimination. In Monahan T (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life.* New York/London: Routledge, 209-224.

Lyon D (2008) Filtering Flows, Friends, and Foes: Global Surveillance. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 29-50.

Lyon D, Haggerty K D and Ball K (2012) Introducing Surveillance Studies. In Ball K, Haggerty K D & Lyon D (eds.) *Routledge Handbook of Surveillance Studies.* Milton Park/New York: Routledge, 1-12.

Magnet S and Rodgers T (2012) Stripping for the State: Whole Body Imaging Technologies and the Surveillance of Othered Bodies. *Feminist Media Studies* 12(1): 101-118.

Manning P K (2006) Reflections on Risk Analysis, Screening, and Contested Rationalities. *Canadian Journal of Criminology & Criminal Justice* 48(3): 453-469.

Manyika J, Chui M, Brown B, Bughin J, Dobbs R, Roxburgh C and Hung Byers A (2011) Big Data: The Next Frontier for Innovation, Competition, and Productivity. Available at: http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx (accessed 7 July 2014). McKinsey Global Institute.

Marquis G (2003) Private Security and Surveillance: From the "Dossier Society" to Database Networks. In Lyon D (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London/New York: Routledge, 226-248.

Martin L and Simon S (2008) A Formula for Disaster: The Department of Homeland Security's Virtual Ontology. *Space and Polity* 12(3): 281-296.

Martin L L (2010) Bombs, Bodies, and Biopolitics: Securitizing the Subject at the Airport Security Checkpoint. *Social & Cultural Geography* 11(1): 17-34.

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

Marx G T and Muschert G W (2007) Personal Information, Borders, and the New Surveillance Studies. *Annual Review of Law and Social Science* 3(1): 375-395.

Massumi B (2002) *Parables for the Virtual: Movement, Affect, Sensation.* Durham/London: Duke University Press.

Massumi B (2005) Fear (The Spectrum Said). *Positions* 13(1): 31-48.

Massumi B (2007) Potential Politics and the Primacy of Preemption. *Theory & Event* 10(2).

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

McCarthy D R (2013) Technology and 'the International' or: How I Learned to Stop Worrying and Love Determinism. *Millennium - Journal of International Studies* 41(3): 470-490.

McCue C (2007) *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis.* Burlington/Oxford: Elsevier.

McLay L A, Jacobson S H and Kobza J E (2006) A multilevel passenger screening problem for aviation security. *Naval Research Logistics* 53(3): 183-197.

McLay L A, Lee A J and Jacobson S H (2010) Risk-Based Policies for Airport Security Checkpoint Screening. *Transportation Science* 44(3): 333-349.

Molotch H (2012) *Against Security: How We Go Wrong at Airports, Subways, and other Sites of Ambigious Danger.* Princeton/Oxford: Princeton University Press.

Monahan T (2006a) Questioning Surveillance and Security. In Monahan T (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life.* New York/London: Routledge, 1-23.

Monahan T (ed.) 2006b. *Surveillance and Security: Technological Politics and Power in Everyday Life,* New York/London: Routledge.

Monahan T (2009) Dreams of Control at a Distance: Gender, Surveillance, and Social Control. *Cultural Studies ↔ Critical Methodologies* 9(2): 286-305.

Monahan T (2010) Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance. In Haggerty K D & Samatas M (eds.) *Surveillance and Democracy.* Milton Park/New York: Routledge, 91-110.

Mordini E (2010) ANNEX I: Policy Brief on: Whole Body - Imaging at Airport Checkpoints: The Ethical and Policy Context (updated March 2011). In von Schomberg R (ed.) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields.* Brussels: European Commission, 165-209.

Morgenthau H J (1948) *Politics Among Nations: The Struggle for Power and Peace.* New York: Knopf.

Mulkay M (1988) *On Humor: Its Natur and Place in Modern Society.* Cambridge: Polity Press.

Muller B (2009) Borders, Risks, Exclusions. *Studies in Social Justice* 3(1): 67-78.

Murakami Wood D, Konvitz E and Ball K (2003) The Constant State of Emergency?: Surveillance after 9/11. In Ball K & Webster F (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age.* London/Sterling: Pluto Press, 137-150.

Nagenborg M (2009) Ethik als Partner in der Technikgestaltung. In Maring M (ed.) *Verantwortung in Technik und Ökonomie.* Karlsruhe: Universitätsverlag Karlsruhe, 101-116.

Nagenborg M (2011) Körperscanner. In Maring M (ed.) *Fallstudien zur Ethik in Wissenschaft, Wirtschaft, Technik und Gesellschaft.* Karlsruhe: KIT Scientific Publishing.

Neal A W (2009) Securitization and Risk at the EU Border: The Origins of FRONTEX. *Journal of Common Market Studies* 47(2): 333-356.

Neocleous M (2008) *Critique of Security.* Edinburgh: Edinburgh University Press.
Nielsen M M (2011) On Humour in Prison. *European Journal of Criminology* 8(6): 500-514.
Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford Law Books.
Norrick N R and Spitz A (2008) Humor as a Resource for Mitigating Conflict in Interaction. *Journal of Pragmatics* 40(10): 1661-1686.
O'Malley P (2000) Introduction: Configurations of Risk. *Economy and Society* 29(4): 457-459.
O'Malley P (2004) *Risk, Uncertainty and Government.* London: The GlassHouse Press.
O'Malley P (2006) Risks, Ethics, and Airport Security. *Canadian Journal of Criminology and Criminal Justice* 48(3): 413-421.
Official Journal of the European Communities (1995) 95/46/EC. Directive of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Brussels.
Ogus A (2004) W(h)ither the Economic Theory of Regulation? What Economic Theory of Regulation? In Jordana J & Levi-Faur D (eds.) *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance.* Cheltenham/Northhampton: Edward Elgar, 31-44.
Osborne D and Gaebler T (1993) *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector.* New York: Penguin Books.
Pallitto R M and Heyman J (2008) Theorizing Cross-Border Mobility: Surveillance, Security and Identity. *Surveillance & Society* 5(3): 315-333.
Palmer J (1994) *Taking Humour Seriously.* London/New York: Routledge.
Paolucci P and Richardson M (2006) Sociology of Humor and a Critical Dramaturgy. *Symbolic Interaction* 29(3): 331-348.
Poole R W, Jr. (2009) Towards a Risk-based Aviation Security Policy. In OECD & ITF (eds.) *Terrorism and International Transport: Towards Risk-based Security Policy.* Paris: OECD.
Redden S M and Terry J (2013) The End of the Line: Feminist Understandings of Resistance to Full-Body Scanning Technology. *International Feminist Journal of Politics* 15(2): 234-253.
Regan P M (2011) Response to Bennett: Also in Defence of Privacy. *Surveillance & Society* 8(4): 497-499.
Rhodes R A W (2007) Understanding Governance: Ten Years On. *Organization Studies* 28(8): 1243-1264.
Rigakos G S and Greener D R (2000) Bubbles of Governance: Private Policing and the Law in Canada. *Canadian Journal of Law and Society* 15(1): 145-185.
Robin C (2004) *Fear: The History of a Political Idea.* Oxford: Oxford University Press.
Rose N (1999) *Powers of Freedom: Reframing Political Thought.* Cambridge: Cambridge University Press.
Rouvroy A (2013) The End(s) of Critique: Data-behaviourism vs. Due-process. In Hildebrandt M & de Vries K (eds.) *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology.* Milton Park/New York: Routledge, 143-168.
Salter M B (2004) Passports, Mobility, and Security: How Smart Can the Border Be? *International Studies Perspectives* 5(1): 71-91.
Salter M B (2007) Governmentalities of an Airport: Heterotopia and Confession. *International Political Sociology* 1(1): 49-66.
Salter M B (2008a) The Global Airport: Managing Space, Speed, and Security. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 1-28.
Salter M B (2008b) Imagining Numbers: Risk, Quantification, and Aviation Security. *Security Dialogue* 39(2-3): 243-266.
Salter M B (2008c) Introduction: Airport Assemblage. In Salter M B (ed.) *Politics at the Airport.* Minneapolis/London: University of Minnesota Press, 1-28.
Salter M B (2008d) Political Science Perspectives on Transportation Security. *Journal of Transportation Security* 1(1): 29-35.
Salter M B (ed.) 2008e. *Politics at the Airport,* Minneapolis/London: University of Minnesota Press.

Salter M B (2008f) Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development* 11(4): 321-349.

Salter M B (2011a) "No Joking!". In Bajc V & de Lint W (eds.) *Security and Everyday Life.* New York/London: Routledge, 31-49.

Salter M B (2011b) When Securitization Fails: The Hard Case of Counter-terrorism Programs. In Balzacq T (ed.) *Securitization Theory: How Security Problems Emerge and Dissolve.* Milton Park/New York: Routledge, 116-132.

Salter M B (2013) To Make Move and Let Stop: Mobility and the Assemblage of Circulation. *Mobilities* 8(1): 7-19.

Sanders T (2004) Controllable Laughter: Managing Sex Work Through Humour. *Sociology* 38(2): 273-291.

Schaar P (2010) Privacy by Design. *Identity in the Information Society* 3(2): 267-274.

Schmitt C (1922) *Politische Theologie: Vier Kapitel zur Lehre von der Souveränität.* München/Leipzig: Duncker & Humblot.

Schneier B (2006) *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* New York: Springer.

Schouten P (2014a) Security as Controversy: Reassembling Security at Amsterdam Airport. *Security Dialogue* 45(1): 23-42.

Schouten P (2014b) Security in Action: How John Dewey Can Help Us Follow the Production of Security Assemblages. In Acuto M & Curtis S (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations.* Basingstoke/New York: Palgrave Macmillan, 83-90.

Schreurs W, Hildebrandt M, Kindt E and Vanfleteren M (2008) Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 241-270.

Seidenstat P (2004) Terrorism, Airport Security, and the Private Sector. *Review of Policy Research* 21(3): 275-291.

Shearing C (2006) Reflections on the Refusal to Acknowledge Private Governments. In Wood J & Dupont B (eds.) *Democracy, Society and the Governance of Security.* Cambridge: Cambridge Univ. Press, 11–32.

Shearing C and Stenning P C (1983) Private Security: Implications for Social Control. *Social Problems* 30(5): 493-506.

Shearing C and Wood J (2003a) Governing Security for Common Goods. *International Journal of the Sociology of Law* 31(3): 205-225.

Shearing C and Wood J (2003b) Nodal Governance, Democracy, and the New 'Denizens'. *Journal of Law & Society* 30(3): 400-419.

Solove D J (2008) *Understanding Privacy.* Cambridge/London: Harvard University Press.

Stalder F (2011) Autonomy beyond Privacy? A Rejoinder to Bennett. *Surveillance & Society* 8(4): 508-512.

Starkie D (2002) Airport Regulation and Competition. *Journal of Air Transport Management* 8(1): 63-72.

Steeves V (2009) Reclaiming the Social Value of Privacy. In Kerr I, Steeves V & Lucock C (eds.) *Lessons from the Identity Trail.* Oxford: Oxford University Press, 191-208.

Stengel L and Nagenborg M (undated) Reconstructing European Ethics. How does a Technology Become an Ethical Issue at the Level of the EU? ETICA Deliverable 3.2.2 Annex I.

Stritzel H (2007) Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations* 13(3): 357-383.

Sweet K M (2009) *Aviation and Airport Security. Terrorism and Safety Concerns.* Boca Raton/London/New York: CRC Press.

Székely I, Szabó M D and Vissy B (2011) Regulating the Future? Law, Ethics, and Emerging Technologies. *Journal of Information, Communication and Ethics in Society* 9(3): 180-194.

Szyliowicz J S (2004) Aviation Security: Promise or Reality? *Studies in Conflict and Terrorism* 27(1): 47-63.

Taureck R (2006) Securitization Theory and Securitization Studies. *Journal of International Relations and Development* 9(1): 53-61.

Thatcher S (2008) Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector - Reply. In Hildebrandt M & Gutwirth S (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht/London: Springer Science + Business Media B.V., 264-270.

Tiessen M (2011) Being Watched Watching Watchers Watch: Determining the Digitized Future While Profitably Modulating Preemption (at the Airport). *Surveillance & Society* 9(1/2): 167-184.

TSA (2013) The TSA Blog, 18 January 2013: Rapiscan Backscatter Contract Terminated – Units to be Removed, http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract.html (accessed 7 July 2014).

Tsoukala A (2010) Risk-focused Security Policies and Human Rights. The Impossible Symbiosis. In Salter M B (ed.) *Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror.* London/New York: Routledge, 41-59.

Tugas J F (2013) Privacy and Body Scanners at EU Airports. *Novática* Special English Edition(2012/2013 Annual Selection of Articles): 49-54.

Valkenburg G (2014) The Trade-Off Model Between Privacy and Security From a Sociotechnical Perspective. Paper presented at Computers, Privacy and Data Protection Conference, Brussels, 22-24 January.

Valverde M and Mopas M (2004) Insecurity and the Dream of Targeted Governance. In Larner W & Walters W (eds.) *Global Governmentality. Governing International Spaces.* Milton Park/New York: Routledge, 233-250.

van Lieshout M, Friedewald M, Wright D and Gutwirth S (2013) Reconciling Privacy and Security. *Innovation: The European Journal of Social Science Research* 26(1/2): 119-132.

van Otterlo M (2013) A Machine Learning View on Profiling. In Hildebrandt M & de Vries K (eds.) *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology.* Milton Park/New York: Routledge, 41-64.

Wæver O (1995) Securitization and Desecuritization. In Lipschutz R D (ed.) *On Security.* New York/Chichester: Columbia University Press, 46-86.

Wæver O (2004) Aberystwyth, Paris, Copenhagen. New 'Schools' in Security Theory and Their Origins Between Core and Periphery. Paper presented at International Studies Association Annual Conference, Montreal, 17-20 March.

Wæver O and Buzan B (2007) After the Return to Theory: The Past, Present, and Future of Security Studies. In Collins A (ed.) *Contemporary Security Studies.* Oxford/New York: Oxford University Press, 393-410.

Waldron J (2003) Security and Liberty: The Image of Balance. *Journal of Political Philosophy* 11(2): 191-210.

Walt S M (1991) The Renaissance of Security Studies. *International Studies Quarterly* 35(2): 211-239.

Walters W (2012) *Governmentality: Critical Encounters.* Milton Park/New York: Routledge.

Warren S D and Brandeis L D (1890) The Right to Privacy. *Harvard Law Review* 4(5): 193-220.

Westin A F (1970) *Privacy and Freedom.* New York: Atheneum.

Westin A F (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues* 59(2): 431-453.

White A (2012) The New Political Economy of Private Security. *Theoretical Criminology* 16(1): 85-101.

Williams M C (2011) The Continuing Evolution of Securitization Theory. In Balzacq T (ed.) *Securitization Theory: How Security Problems Emerge and Dissolve.* Milton Park/New York: Routledge, 212-222.

Winner L (2006) Techniques of Preparedness. In Monahan T (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life.* New York/London: Routledge, 275-291.

Wood J and Dupont B (eds.) 2006a. *Democracy, Society and the Governance of Security,* Cambridge: Cambridge Univ. Press.

Wood J and Dupont B (2006b) Introduction: Understanding the Governance of Security. In Wood J & Dupont B (eds.) *Democracy, Society and the Governance of Security.* Cambridge: Cambridge Univ. Press, 1-10.

Wright D (2011) A Framework for the Ethical Impact Assessment of Information Technology. *Ethics and Information Technology* 13(3): 199–226.

Wyn Jones R (ed.) 2001. *Critical Theory & World Politics,* Boulder/London: Lynne Rienner Publishers.

Yar M (2011) From the 'Governance of Security' to 'Governance Failure': Refining the Criminological Agenda. *Internet Journal of Criminology*.

Zarsky T Z (2011) Governmental Data Mining and its Alternatives. *Penn State Law Review* 116(2): 285-330.

Zedner L (2006a) Liquid Security: Managing the Market for Crime Control. *Criminology and Criminal Justice* 6(3): 267-288.

Zedner L (2006b) Neither Safe Nor Sound? The Perils and Possibilities of Risk. *Canadian Journal of Criminology & Criminal Justice* 48(3): 423-434.

Zedner L (2007) Pre-crime and post-criminology? *Theoretical Criminology* 11(2): 261-281.

Zijderveld A C (1968) Jokes and Their Relation to Social Reality. *Social Research* 35(2): 286-311.

Zureik E and Hindle K (2004) Governance, Security, and Technology: The Case of Biometrics. *Studies in Political Economy* 73: 113-137.