Special issue on Preemption, Practice, Politics

SECURITY DIALOGUE

Security Dialogue
2014, Vol. 45(5) 494–511

DOI: 10.1177/0967010614544204
sdi.sagepub.com
SAGE

The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union

Matthias Leese
International Centre for Ethics in the Sciences and Humanities (IZEW), University of Tuebingen, Germany

Abstract
This article argues that with increasingly large databases and computational power, profiling as a key part of security governance is experiencing 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 those of traditional profiling. While several scholars have dealt with the consequences of black-boxed and invisible algorithmic analytics in terms of privacy and data protection, this article 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 article 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, leading to a diminishing role of the tools of the anti-discrimination framework.

Keywords
critical theory, European Union, Foucault, security, terror, profiling

Introduction

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 policymaking, the European Union has recently fostered trends in intelligence collection, analytics, and predictive data mining. The Stockholm Programme, the European Council's framework for the period 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: 18–19). This trend has led to an increasing number of

Corresponding author:
Matthias Leese.
Email: matthias.leese@izew.uni-tuebingen.de

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 European Union (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 he or she possibly poses.

Thus, data are 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 widespread areas like insurance (Lobo-Guerrero, 2011), the financial system (De Goede, 2008), 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, 2006; O'Malley, 2006; Salter, 2008). However, a series of questions emerges from the notion of risk and anticipatory governance. As Anderson (2010: 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 article engages the still-pending EU PNR Directive that is set to be one of the cornerstone policy tools of the Stockholm Programme. The proposed system envisages, among other things, making 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 article 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 means of structure exploration and knowledge generation ('induction') (Anrig et al., 2008: 66), the article will examine 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 proactive approaches to processing PNR data (European Commission, 2011a: 3–4). While 'real-time' use essentially enacts traditional profiling practices, the 'proactive' concept, as detailed in the European Commission proposal, explicitly aims at 'analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments' (European Commission, 2011a: Art. 4.2d), 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). The PNR Directive appears as an attempt to build on such temporary hypotheses to enable action against unpredictable threats, rendering them knowledgeable through large-scale analytics. Connecting those findings to Foucauldian thought on modes of governance eventually enables the analysis to demonstrate how new modes of knowledge creation impact the reassembling 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 who engage with PNR data concentrate on issues of privacy and data protection (Bellanova and Duez, 2012; Bennett, 2005; De Hert and Bellanova, 2011). 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 (Cheney-Lippold, 2011; Gandy, 1993, 2010). This article thus seeks to reconnect theoretical insights into profiling with empirical evidence from EU security policymaking, and thereby to offer a conceptualization of the changing

landscape of security governance. In the vein of preemption, it engages the institutionalization and routinization of speculative futures. It concludes that with the ongoing emergence of data-driven profiling, the legal toolbox of the anti-discrimination framework suffers an increasing ineffectiveness. Owing to the increasing use of dynamic algorithmic systems, possible cases of discrimination will be less visible and traceable, leading to diminishing accountability. In other words, preemption renders its own benchmarks fluid, with the result that they perpetually escape the grasp of legal protection standards.

Aviation, risk, and PNR data

The aviation sector has been framed as a particularly perfect fit for anticipatory governance, both on account of its highly symbolic role in the attacks of 9/11 and the ensuing 'war on terror', and owing to the applicability of the concept of risk in checkpoint-centered screening operations (Leese, 2013). In the spatial bottleneck of the checkpoint, the passenger flow becomes slowed down for the purpose of thorough scrutiny and regulation of access to the secured sectors of the airport (Jones, 2009). The deployment of risk profiling in this context promises to enact preemption in terms of reallocating 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 consequently prone to producing exceptionally high numbers of Type I errors (false positives). This phenomenon 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 individuals incorrectly flagged as being high-risk 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, owing both to time constraints on the practical level and to the dichotomous logic of suspicion/non-suspicion in security screening.

Still, on several recent occasions, representatives from the aviation sector have called for more risk-oriented security policies, as, for instance, during the European Commission's High Level Conference on 'Protecting Civil Aviation Against Terrorism' (European Commission, 2011b) and the International Civil Aviation Organization's High Level Conference on Aviation Security (ICAO, 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 as one of the most important policy tools in fighting terrorism and transnational crime that was envisioned to be implemented until 2014.

Such an EU PNR system has a long political history by now, and its status remains unresolved for the time being. The Commission's original proposal from 2007 (European Commission, 2007), 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 on 1 December 2009, which resulted in the dissolution of the former EU pillar structure. However, as PNR data were 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 (European Commission, 2011a). On 23 April 2012, the European Council (2012) also presented a further advanced proposal. The Commission's proposal was eventually forwarded to the Civil Liberties Committee, which rejected it with a vote of 30 to 25 on 24 April 2013.[1] 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.[2] The fact that a European PNR system is regarded as one of the core policy tools in the Stockholm Programme and the persistence of the Commission with regard to the proposal make it possible that a (revised) version of the proposal could be decided upon in a plenary vote in the European Parliament, thus increasing the chances for an adoption. In any case, it seems probable that the plans for such an EU PNR system will not be crossed off the agenda easily.

What, then, makes PNR data so valuable? 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 his or her 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 (European Council, 2012: Annex II). Thus, almost naturally, PNR data have 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 USA on 28 May 2004 (with subsequent agreements in 2007 and 2011) turned the data into a resource for security operations by the US Department of Homeland Security and 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-in to obtain passenger data from all intra-EU flights (European Council, 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. 4.2a), 'against relevant databases, including international or national databases or national mirrors of Union databases' (Art. 4.2b), 'on a case-by-case basis, to duly reasoned requests from competent authorities' (Art. 4.2c), as well as 'for the purpose of updating or creating new criteria for carrying out assessments' (Art. 4.2d). 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 proactive creation of new assessment criteria as defined in Article 4.2d. This explicit scope highlights the significance of PNR data for new modes of data-driven profiling.

Theorizing profiling

Profiling is a powerful technique that is currently experiencing major changes related to the way in which knowledge about populations and futures is created. In post-9/11 security regimes, the efforts of policymakers 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 defense Donald Rumsfeld's statement about 'unknown unknowns' in a speech at NATO's headquarters on 6 June 2002.[3] 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 in 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, which is still ontologically 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 than for the doubt it insinuates' (Ewald, 2002: 274). Precaution embraces contingency by moving beyond risk as a calculable objectification; however, it appears to be 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 the concept's earlier use in environmental protection (Aradau and Van Munster, 2007; Beck, 2002). Anderson (2010: 792) thus adds that precautionary measures seek to act before an identified threat reaches a point of irreversible damage, and thus distinguishes precaution from preemptive measures. Preemption, as it 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, 2010: 792).

With the threat in the current EU security agenda being predominantly defined as terrorism and serious crime, traditional forms of profiling, according to 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 (Amoore, 2013) 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 later, the construction of the profile consequently 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 within the scope of the legal tools of the non-discrimination framework owing to its static nature, while the latter manages to constantly escape the current regulatory regimes owing 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 predefined 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 sections of 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: 47–48). In terms of the 'war on terror', the debate on post-9/11 racial profiling against Muslims bears witness to such discriminatory practices (Harcourt, 2007; Harris and Schneier, 2012). Indeed, as Zedner (2006: 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: 326–327), thus risk connects economic status to enhanced mobility. And, while Adey (2008) emphasizes that mobility has always carried a strong notion of inequality, with airports being genuine 'difference machines', '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 pitfalls 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. Consequently, policymakers have been careful to implement anti-discriminatory safeguards into profiling regimes.

Profiling and non-discrimination

The principle of non-discrimination – also referred to as the 'principle of equality' or the 'non-discrimination clause' (Edel, 2010: 8–9) – has been expressed as one of the cornerstone 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 Article 21 of the Charter of Fundamental Rights of the European Union, in Article 14 (and Article 1 of Protocol No. 12) of the European Convention on Human Rights, and in Articles 18–25 of the Treaty on the Functioning of the European Union. More specifically, the EU legal framework is composed of several directives that implement the non-discriminatory treatment of persons, but focus primarily on labor market issues (Gellert et al., 2013: 68). The rather fragmented nature of this field is set to be transformed 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 currently applicable in the EU 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 (European Parliament/European Council, 1995). This focus 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 the document points out, the construction of profiles from PNR data is subject to 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. (European Council, 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' (European Council, 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 and states 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' (European Council, 2012: Art. 11.1), thus providing a legal toolbox for the challenge of discriminatory issues on the individual level.

As will become apparent throughout the remainder of this article, however, 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 predefined 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, according to the reading I put forward, can be best understood through a Foucauldian framework of governmentality. 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 1976–1979, 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). This is essentially the practice that Haggerty and Ericson (2000) 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 reassemble them for distinct purposes. With regard to unfolding its normalizing power, discipline then proceeds by forcing the disassembled individual to conform to a model of desired behavior and desired characteristics. As Foucault (2007: 57) emphasizes, 'it is not the normal and the abnormal that is fundamental and primary disciplinary power, it is the norm'. 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' (European Council, 2012: Art. 4.2a). Thus, when a representation of the predefined profile is found in the database, the corresponding individual will 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.

In his analysis of contemporary security governmentality, however, 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 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, 2010: 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 previously not been accessible. 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 a 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 owing to constraints in actual knowledge about terrorists and criminals, data-driven analytics go beyond the limits of the known and seek to unveil and rationalize the unknown. Not only do they seek to render the future actionable, they also promise to provide a glimpse into the future by creating a new and distinct form of knowledge about it.

Although Anderson (2010: 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 of detecting 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 allow not only 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 on the basis of 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 retranslated into interpretations of the real world in the form of *temporary* profiling hypotheses. In contrast 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 reassembly 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 might not be particularly meaningful. 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 decisionmaking 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 shown further, 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. Through the imposition of 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 may possibly be canceled out. However, with data-driven analytics, this is not the case. While the starting point remains 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 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?' (De Vries, 2010: 81, emphasis in original).

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. The truth of the machine 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 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 germination' (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). In contrast to deterministic types of algorithms that produce the same result over and over when run against the same database and that 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 owing 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 rely either 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 understood as a clear-cut analytical scheme, though. On the contrary, it appears more appropriate to interpret the distinction between traditional and data-driven profiling in terms of the construction of Weberian ideal types. The artificial superelevation of disciplinary versus 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 (2007: 8) 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'. Such a conceptualization of overlapping modes can clearly be found in the PNR proposal, as it seeks to deploy traditional 'real-time' (Art. 4.1a)

and data-driven 'proactive' (Art. 4.1d) types of profiling in a parallel fashion, and moreover combine them with checks against remote databases and individual in-depth scrutiny. As Collier (2009: 79) emphasizes, the scope for any enquiry 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'. Accordingly, an analysis of how profiling practices enact power over mobile populations in the name of the 'war on terror' 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). If we understand 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 article 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 notice when he or she becomes 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'. However, in the case of data-driven profiling, the occurrence of discrimination will be based not 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. Nonetheless, 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 posteriori. 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 (European Council, 2012: 16). However, this is a deceptive safeguard, as data-driven profiling in security screening relies on the

assumption that all revealed patterns must necessarily be scrutinized in order to ascertain 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 reviewers lose 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 with 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 relocated into the 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*. (emphasis in original)

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

Given the above, and assuming that apparatuses of security always possess a strategic notion (Dillon, 2010: 63), what can we learn from the reassembly 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 owing to the non-applicability of its tools. We encounter a tension between the law and 'normality', as normality no longer derives from a static norm but is constantly reconfigured. 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 contestation, but rather must be reconnected to the real world in order to cancel out the possibilistic mode of threat (Amoore, 2013) 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 no longer the central focus of interest, but that categories are the new way of coping 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 predefined 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 who 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 changing 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 reassembled and recombined. 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 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: 10)

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 article has sought to critically engage 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 a European PNR system have been rendered as cornerstones for providing European law enforcement agencies with the tools to fight terrorism and crime through new forms of future-related governance. Such data-driven security practices not only imply practical consequences, but also relate to the theoretical framing of changing security regimes. This article has connected Foucauldian thought on 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 EU's non-discrimination framework. Despite the article's 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 of 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 reassembles 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 are 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 of 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 generation will be found on broader levels. Thus, can the non-discrimination framework and data-driven profiling be reconciled in such a way 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 reopen 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 introduce more black boxes, which when subsequently opened simply introduce 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 reopen 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, owing 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) not very 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 reassembled and recombined 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 … 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.

Acknowledgements

Previous versions of this article were presented at the 'Anticipate and Preempt' workshop in Amsterdam, 4–5 March 2013; at the 'National Security, Risk Management, and the Transformation of Bureaucratic Ethics'

conference in Copenhagen, 23–24 May 2013; and at the 4S Annual Meeting in San Diego, 9–12 October 2013. The author is grateful for all feedback and remarks received on those occasions, and particularly for comments by Thomas Diez and Stefano Guzzini.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes

1. See http://www.europarl.europa.eu/news/en/news-room/content/20130422IPR07523/html/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal (accessed 12 December 2013).
2. See http://euobserver.com/justice/119926 (accessed 12 December 2013).
3. See http://www.nato.int/docu/speech/2002/s020606g.htm (accessed 12 December 2013).

References

Adey P (2008) Mobilities and modulations: The airport as a difference machine. In: Salter MB (ed.) *Politics at the Airport*. Minneapolis, MN and London: University of Minnesota Press, pp. 145–160.

Airports Council International/Association of European Airlines (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 30 April 2014).

Amoore L (2006) Biometric borders: Governing mobilities in the War on Terror. *Political Geography* 25(3): 336–351.

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, NC and 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.

Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

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 July. Available at: http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory.

Anrig B, Browne W and Gasson M (2008) The role of algorithms in profiling. In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-disciplinary Perspectives*. Dordrecht/London: Springer Science/Business Media BV, pp. 65–88.

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.

Ayres I (2007) *Super Crunchers: Why Thinking-by-Numbers Is the New Way To Be Smart*. New York: Bantam.

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.

Bennett CJ (2005) What happens when you book an airline ticket? The collection and processing of passenger data post-9/11. In: Zureik E and Salter MB (eds) *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton and Portland, OR: Willan, pp. 113–138.

Boyle P and Haggerty KD (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.

Brownsword R (2008) Knowing me, knowing you: Profiling, privacy and the public interest. In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-disciplinary Perspectives*. Dordrecht/London: Springer Science/Business Media BV, pp. 345–364.

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.

Collier S J (2009) Topologies of power: Foucault's analysis of political government beyond 'governmentality'. *Theory, Culture & Society* 26(6): 78–108.

De Goede M (2008) Money, media and the anti-politics of terrorist finance. *European Journal of Cultural Studies* 11(3): 289–310.

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 Vries K (2010) Identity, profiling algorithms and a world of ambient intelligence. *Ethics and Information Technology* 12(1): 71–85.

Deleuze G (1992) Postscript on the societies of control. *October* 59: 3–7.

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 30 April 2014).

Dillon M (2010) Biopolitics of security. In Burgess JP (ed.) *The Routledge Handbook of New Security Studies*. Milton Park and New York: Routledge, pp. 61–71.

Dillon M and Lobo-Guerrero L (2008) Biopolitics of security in the 21st century: An introduction. *Review of International Studies* 34(2): 265–292.

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

European Commission (2007) *Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, 6 November 2007*. COM(2007) 654 final. Brussels: European Commission.

European Commission (2008) *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 2008*. COM(2008) 426 final. Brussels: European Commission.

European Commission (2011a) *Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, 2 February 2011*. COM(2011) 32 final. Brussels: European Commission.

European Commission (2011b) 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 30 April 2014).

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

European Council (2012) *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*. 8916/12. Brussels: Council of the European Union.

European Parliament/European Council (1995) *Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 24 October. 95/46/EC. *Official Journal of the European Communities*. Brussels: European Parliament and European Council.

Ewald F (2002) The return of Descartes's malicious demon: An outline of a philosophy of precaution. In Baker T and Simon J (eds) *Embracing Risk: The Changing Culture of Insurance and Responsibility*. Chicago, IL and London: University of Chicago Press, pp. 273–301.

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

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

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

Gandy OH (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

Gandy OH (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 and Zarsky T (eds) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*. Heidelberg, New York, Dordrecht and London: Springer, pp. 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 24 June 2014).

Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski P and Foot K (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge, MA: MIT Press, 167–194.

González Fuster G, Gutwirth S and Ellyne E (2010) Profiling in the European Union: A high-risk practice. INEX Policy Brief 10. Available at: http://www.ceps.eu/ceps/dld/3474/pdf (accessed 30 April 2014).

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622.

Hansen HK and Porter T (2012) What do numbers do in transnational governance? *International Political Sociology* 6(4): 409–426.

Harcourt BE (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 BJ and Lazarus L (eds) *Security and Human Rights*. Oxford and Portland, OR: Hart Publishing, pp. 73–98.

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 30 April 2014).

Hildebrandt M (2008) Defining profiling: A new type of knowledge? In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-disciplinary Perspectives*. Dordrecht/London: Springer Science/Business Media BV, 17–46.

Hildebrandt M and Gutwirth S (2008) Concise conclusions: Citizens out of control. In: Hildebrandt M and Gutwirth S (eds) *Profiling the European Citizen: Cross-disciplinary Perspectives*. Dordrecht/London: Springer Science/Business Media BV, 365–368.

International Air Transport Association (IATA) (2011) Checkpoint of the future executive summary. Available at: https://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf (accessed 30 April 2014).

International Civil Aviation Organization (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 30 April 2014).

Introna LD (2013) Algorithms, performativity and governability. Paper presented at the conference 'Governing Algorithms: A Conference On Computation, Automation, and Control', New York University, 16–17 May.

Jones R (2009) Checkpoint security: Gateways, airports and the architecture of security. In: Aas KF, Gundhus HO and Lomell HM (eds) *Technologies of InSecurity: The Surveillance of Everyday Life*. London: Routledge-Cavendish, pp. 81–102.

Leese M (2013) Blurring the dimensions of privacy? Law enforcement and trusted traveler programs. *Computer Law & Security Review* 29(5): 480–490.

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

Lyon D (2006) Airport screening, surveillance, and social sorting: Canadian responses to 9/11 in context. *Canadian Journal of Criminology and Criminal Justice* 48(3): 397–411.

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

McLay LA, Lee AJ and Jacobson SH (2010) Risk-based policies for airport security checkpoint screening. *Transportation Science* 44(3): 333–349.

Manyika J, Chui M, Brown B, et al. (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 30 April 2014).

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.

Matzner T (2013) The model gap: Cognitive systems in security applications and their ethical implications. *AI & Society*. Epub ahead of print 5 November 2013. DOI:10.1007/s00146–013–0525–4.

Muller B (2009) Borders, risks, exclusions. *Studies in Social Justice* 3(1): 67–78.

O'Malley P (2006) Risks, ethics, and airport security. *Canadian Journal of Criminology and Criminal Justice* 48(3): 413–421.

Pallitto R and Heyman J (2008) Theorizing cross-border mobility: Surveillance, security and identity. *Surveillance & Society* 5(3): 315–333.

Rouvroy A (2013) The end(s) of critique: Data-behaviourism vs. due-process. In: Hildebrandt M and De Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Milton Park and New York: Routledge, pp. 143–168.

Salter MB (2004) Passports, mobility, and security: How smart can the border be? *International Studies Perspectives* 5(1): 71–91.

Salter MB (2008) Imagining numbers: Risk, quantification, and aviation security. *Security Dialogue* 39(2–3): 243–266.

Tsoukala A (2010) Risk-focused security policies and human rights: The impossible symbiosis. In: Salter MB (ed.) *Mapping Transatlantic Security Relations: The EU, Canada, and the War on Terror*. London and New York: Routledge, pp. 41–59.

Valverde M and Mopas M (2004) Insecurity and the dream of targeted governance. In: Larner W and Walters W (eds) *Global Governmentality: Governing International Spaces*. Milton Park and New York: Routledge, pp. 233–250.

Zarsky TZ (2011) Governmental data mining and its alternatives. *Penn State Law Review* 116(2): 285–330.

Zedner L (2006) Neither safe nor sound? The perils and possibilities of risk. *Canadian Journal of Criminology & Criminal Justice* 48(3): 423–434.

Matthias Leese is a Research Associate within the Security Ethics section at the International Centre for Ethics in the Sciences and the Humanities (IZEW), University of Tuebingen. His primary research interests are located in the fields of surveillance and security studies, particularly dealing with civil liberties, anticipatory governance, and securitization issues.