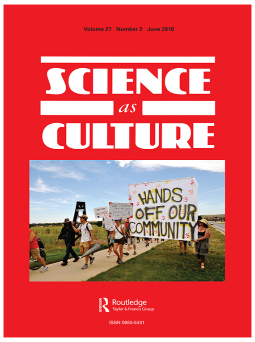

Science as Culture

ISSN: 0950-5431 (Print) 1470-1189 (Online) Journal homepage: http://www.tandfonline.com/loi/csac20

Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences

Sanneke Kloppenburg & Irma van der Ploeg

To cite this article: Sanneke Kloppenburg & Irma van der Ploeg (2018): Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences, Science as Culture, DOI: 10.1080/09505431.2018.1519534

To link to this article: https://doi.org/10.1080/09505431.2018.1519534

Published online: 19 Sep 2018.

SCIENCE AS CULTURE
https://doi.org/10.1080/09505431.2018.1519534

OPEN ACCESS

Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences

Sanneke Kloppenburg[a] and Irma van der Ploeg[b]

[a]Environmental Policy Group, Wageningen University, Wageningen, Netherlands; [b]UNU-MERIT, Maastricht University, Maastricht, Netherlands

ABSTRACT
Worldwide, biometrics are quickly becoming the preferred solution to a wide range of problems involving identity checking. Biometrics are claimed to provide more secure identification and verification, because 'the body does not lie.' Yet, every biometric check consists of a process with many intermediate steps, introducing contingency and choice on many levels. In addition, there are underlying normative assumptions regarding human bodies that affect the functioning of biometric systems in highly problematic ways. In recent social science studies, the failures of biometric systems have been interpreted as gendered and racialized biases. A more nuanced understanding of how biometrics and bodily differences intersect draws attention to how bodily differences are produced, used, and problematized during the research and design phases of biometric systems, as well as in their use. In technical engineering research, issues of biometrics' performance and human differences are already transformed into R&D challenges in variously more and less problematic ways. In daily practices of border control, system operators engage in workarounds to make the technology work well with a wide range of users. This shows that claims about 'inherent whiteness' of biometrics should be adjusted: relationships between biometric technologies, gender and ethnicity are emergent, multiple and complex. Moreover, from the viewpoint of theorizing gender and ethnicity, biometrics' difficulties in correctly recognising pre-defined categories of gender or ethnicity may be less significant than its involvement in *producing and enacting* (new) gender and ethnic classifications and identities.

Keywords
Biometrics; border management; identity; ethnicity; enactment

Introduction

Biometrics—the automated recognition of individuals based on their physical and/or behavioural characteristics such as fingerprints, faces, iris patterns, or

CONTACT Sanneke Kloppenburg sanneke.kloppenburg@wur.nl Environmental Policy Group, Wageningen University, 6708 PB Wageningen, Netherlands

voices—is quickly becoming central to the exercise of citizenship in countries worldwide. With the cost of biometric technology decreasing rapidly and global corporations and donors such as the World Bank promoting the use of biometrics in developing countries, more and more countries start enrolling their entire population in biometric programmes. Some of the largest of these, such as the Indian Unique Identification Project (see e.g. Rao and Greenleaf 2013) include hundreds of millions of people. In Europe, the largest biometric systems are deployed in the areas of migration and border management, and include the Schengen Information System (SIS), the Visa Information System (VIS), and Eurodac. Proposals to improve the management of Europe's external borders—the introduction of an Entry/Exit system (EES) a Registered Traveller Programme (RTP) for third-country nationals, and Automated Border Control for EU citizens—also all rely heavily on the use of biometrics.

Biometrics are believed to provide solutions to a wide range of problems involving identity checking. In the context of national ID programmes in developing countries, biometrics are conceived as a tool for fostering inclusion (Gelb and Clark 2013) and as capable of fixing a failed state infrastructure (Breckenridge 2005). In European border management, there is a dominant discourse that new technologies, including biometrics, can speed up border passage while at the same time making it more secure. Behind these imaginations is the belief that biometrics allow *certain* identification. This certainty results from the presumed unchangeable, unalienable, and unique nature of the individual biometric features that are used, as opposed to tokens, cards, passwords, pins or documents that can be lost, copied, forged, shared, etcetera.

However, in reaction to this increased reliance on and trust in biometrics for securing identity, serious criticisms of these technological practices have been put forward by human rights advocates, data protection authorities, and social scientists. This includes questions about the reliability and security of biometric systems, and their accessibility and usability for different people. A few years ago, the United States National Research Council in a report emphasized that '[n]o biometric technology is infallible; all are probabilistic and bring uncertainty to the association of an individual with a biometric reference […]' (Pato and Millet 2010, p. 52). In addition, the report stated, 'Some individuals may not be able to enroll in a system or be recognized by it as a consequence of physical constraints, and still others may have characteristics that are not distinctive enough for the system to recognize' (Pato and Millet 2010, p. 89). Biometric systems thus appear to be able to cope with human bodily differences only to a certain extent. The increasing reliance on biometrics technologies in areas such as border management, immigration, and law enforcement renders these criticisms acute.

A number of social scientific studies have interpreted the issues related with human bodily differences in terms of racialized and gendered biases (Magnet 2011, Pugliese 2010, Introna and Wood 2004). The aim of the paper is to expand our understanding of the relationships between biometrics and bodily differences by taking an STS inspired perspective that is able to grasp the multiple ways in which biometric systems and their designers and operators *do* bodily differences in practices. In understanding biometric technologies as part of sociotechnical practices of securing identity we are able to highlight that security and accuracy are not inherent to the technology, but something that is achieved (or not) in practice, and involves dealing with bodily differences in multiple ways. Our claim is that rather than biometric technologies failing to read or represent (particular) bodies, biometric technologies enact bodily differences (e.g. Mol and Law 2004, Van der Ploeg 2011, M'Charek 2013). Our main question is: How are bodily differences produced, used, problematized and made (ir)relevant in biometric practices, both during R&D phases and in use?

We examine this question by first introducing a number of key concepts from ANT, and more specifically, material-semiotic approaches that we need for our analysis. Next, we conduct an analysis of techno-scientific literature on biometric performance, to identify how bodily differences emerge in engineers' understanding of performance problems and their subsequent translations (Callon 1984) into R&D challenges. We then turn to two empirical examples of how bodily differences become operationally (in)significant in specific border control contexts. Here we build on material collected as part of our previous work on border technologies at airports (Kloppenburg 2013) and digital identities (Van der Ploeg and Pridmore 2016). The first example comes from a two-week ethnography of one of the authors at an automated border passage programme at an Asian airport. This included joining several work shifts of the programmes' employees at the border, the enrolment centre, and in the back office, as well as interviews with two managers and two technicians of the programme. The second example comes from fieldwork conducted in the context of the DigIDeas project of which the other author was the PI (see LaFors-Owczynik and Van der Ploeg 2016). In the conclusion we discuss the implications this more empirically substantiated, STS-inspired view has for understanding the social and ethical aspects of the use of biometric technologies for identity checking.

Analytical Perspectives on the Politics of Biometric Technologies

One of the attractions of biometrics is that the body is thought to provide an objective and incontrovertible source of truth about a person's identity (Martin and Whitley 2013). An often heard argument of biometrics' advocates is that 'the body does not lie,' and biometric technologies are believed to give direct access to these truths. An STS perspective on biometric technologies, however, does not take this claim for granted, but stresses the opposite. Instead of considering biometric technologies as neutral intermediaries in processes of identity verification, it would emphasize the mutual shaping of technology and context. The context (including for example societal values and normative assumptions) shapes the technology, and at the same time technologies are constitutive of the social, in the sense that they actively shape their own context of use.

In our analysis of biometric technologies and bodily differences, we therefore proceed from the STS view on technology as having both intentional and unintentional in-built values and norms (Akrich 1992, Callon 1984, Latour 1991). By being designed to work in particular ways, technologies play a constitutive role in the organization of social interactions and relations, which renders them inherently normative and constitutive of what usually is called 'the social.' So rather than perceiving biometric technologies as just material machinery or artefacts, we look at them as affording particular *ways of doing things*, such as for example, verifying identities. In this sense they are a constitutive part of particular human practices, and as such best analysed as an socio-material configuration. A biometric recognition result is the outcome of the interaction between human and non-human elements (including hardware, sensors, algorithms, work practices of officers, travellers and their bodies, regulations governing border control, etcetera) in a particular setting. In order to be able to analyse when and how human bodily differences come to play a role in the design and application of biometric systems, we draw on several concepts: normativity, translation, and tinkering. However, before we discuss our use of these concepts, we first briefly explain the process of biometric recognition.

The Process of Biometric Recognition and the Problem of Errors

While most (though not all) biometric systems may present results in a binary mode (pass vs reject) and thereby seem to provide unambiguous answers about human identity, this result is produced in a process that entails many intermediate steps. Looking more closely at the different phases of the biometric recognition process, we can analyse it as a translation of the body into pieces of information that are subsequently processed in order to generate a biometric recognition result.

In order to become biometrically identifiable, a person first needs to *enrol* in a biometric system to create a reference image: a sensor scans a physical characteristic of an individual (e.g. fingertips, iris, face) and generates a digital representation of it, the *captured biometric sample* (sometimes also called the 'raw' biometric data). Some systems take several images at once and pick the best one for further processing, or include software to enhance the captured image to make it fit for processing. Subsequently this initial dataset is transformed via algorithms into a *biometric template.* This template contains only the information needed to run the pattern recognition algorithm, e.g. a certain number of key comparison points (a *feature set, produced by feature extraction software*). The biometric template is stored in a database or on a token (e.g. a chip on a smart card), together with some identifying information of the person (e.g. a name, visa number).

After this enrolment, a person can, on a later occasion, present themselves for biometric *verification*. In this recognition phase, a sensor device again captures a digital representation of the person's biometric characteristic, which the system transforms via the same algorithms into a second feature set, the *biometric probe*, to compare this with the features of the stored template(s). The resulting *comparison score* is the measured degree of similarity between the biometric probe and biometric template. If the comparison score is above a certain *threshold,* the person presenting herself is recognized by the system (Jain et al. 2011).

It is important to keep in mind how in this whole process, with its many intermediate steps, unavoidably information is lost, filtered, transformed, and new information is produced. Right at the initial data capture by the sensor, only parts of the signal count as information, while what the biometrics literature refers to as noise may be neglected. Many contingent factors further influence the process and shape its outcome, such as what is termed the quality of the algorithm and that of the biometric reference template, and, in the case of 1:n matching *(identification*), the very size of the reference database (Pato and Millet 2010). The result of biometric recognition is therefore not a binary yes/no answer, but a *comparison score*, which is a calculation of the *degree* of similarity. Thus, the process of biometric recognition is best understood as a process of informatization of the body, where each step in this process introduces a certain extent of contingency, and, hence, room for deviation and error (Van der Ploeg and Sprenkels 2011).

In biometric discourse, such failures and errors are described with concepts such as failure to enrol, failure to capture, false acceptance, and false rejection. A *failure to capture* occurs when 'a particular sample provided by the user during authentication cannot be acquired or processed reliably'. The *failure to enrol (FTE) rate* refers to 'the proportion of users that cannot be successfully enrolled in a biometric system' (Jain et al 2011, p. 22.) A *false acceptance* occurs when two samples from different individuals are incorrectly recognized as a match, while a *false rejection* happens when two samples of the same biometric trait of an individual are not recognized as a match (Jain et al 2011, p. 17).

Normative Assumptions in Biometrics

In biometric recognition practices, errors and uncertainties do not emerge randomly, but appear to interact with human bodily differences in several ways. One way in which biometrics and bodily differences intersect has to do with the normative assumptions about human bodies that are embedded in biometric systems (Van der Ploeg 2011). Underlying biometric recognition is an assumption that everybody has *unique* bodily characteristics, but at the same time there is an assumption that everyone is *similar,* in the sense that every human person is assumed to have a clearly audible voice, a set of ten fingerprints, two irises, and a recognizable face, and so on.

With respect to the human bodily features used in biometrics, this means that there is an assumption of *normality* that is defined as the range of variation of human bodily features a system can cope with. Such notions of normality are built into the equipment: hand scanners have particular sizes and shapes, with designated places to put the fingers; fingerprint systems are designed for the registration and comparison of a particular number of fingerprints per individual, cameras to scan faces may be directed at a specific height or optimized for particular light and colour ranges, and the accompanying face recognition software often works best for a particular shade range of skin colour, and so on (Van der Ploeg 2011).

Next to the assumptions about uniqueness and similarity, there is an additional assumption regarding the *stability* of the body over time. In the real world of living organisms, however, bodily features change over time: fingerprints become worn (in particular those of manual workers), faces age, and factors like weight loss or gain, (plastic) surgery, disease, scarring or injury all challenge the assumption of the body's stability over time.

Biometric systems also presuppose a particular *availability* of the user and their body (Van der Ploeg 2011). The acquisition of images requires bodies to be presented, positioned and behave in particular ways, for example to press fingertips on a scanner, stand still for some time, uncover faces, or look straight into a camera without blinking or smiling. In other words, as part of a wider socio-material configuration, technologies usually require different sets of specific users with prescribed behaviours, and a set of assumed characteristics, goals, beliefs, and interests to be operated correctly.

Biometric Technologies and the (re)production of Human Bodily Differences

Earlier social scientific studies on the use of biometric technologies for securing identity have emphasized how these technologies tie identity to the body in specific ways, leading to an informatization of the body (Van der Ploeg 2003), or to the body becoming a password (Aas 2006), or the carrier of the border (Amoore 2006). Surveillance studies (e.g. Lyon 2008) and critical security studies (e.g. Muller 2013) often discuss biometrics by focusing on how biometric technologies and databases are used in order to facilitate or impede the movement of people across borders, and the social and political implications this has. These studies generally pay less attention to the technical and operational details of biometric recognition processes.

A small number of social scientific studies have taken up the challenge of opening the black-box of biometric recognition. Introna and Nissenbaum (2010, p. 4) in their study of facial recognition technologies stress that 'the selection and composition of images that are used to develop FRT algorithms are crucial in shaping the eventual performance of the system'. Media scholar Shoshana Magnet argues that the problems with biometric technologies include their 'disproportionate failure on othered bodies' (Magnet 2011, p. 32). She gives examples of how biometric technologies more often fail with elderly persons, people with disabilities, people of colour, and, in the case of fingerprinting, manual workers. In seeking to explain how biometrics systems come to generate these effects, Magnet suggests that designers rely upon 'erroneous biological understandings of race and gender in the development of biometric technologies' (Magnet 2011, p. 49), and that 'cultural assumptions about othered bodies […] are both explicitly and implicitly coded into the technologies' (Magnet 2011, p. 50).

Whereas Magnet approaches the intersections between biometric technologies and (inequalities of) race, gender, and age in a very generalizing sense, cultural theorist Joseph Pugliese takes the specific biometric sub-process of capturing an image, and investigates its relations to race. His focus is on those instances in which biometric systems 'fail to capture' an image because of the subject's race. He argues that 'a number of these capturing technologies are *infrastructurally calibrated to whiteness* [original emphasis]' (Pugliese 2010, p. 57). In other words 'whiteness is configured as the universal gauge that determines the technical settings and parameters for the visual imaging and capture of a subject' (Pugliese 2010). The camera settings for lighting, for example, may be optimized for white-skinned subjects, making the acquisition of the features of non-white subjects more difficult. Pugliese's argument is not that infrastructural whiteness is the result of racist thinking in the design phase, but rather that it is often *unintentional* and *hidden*.

Selective Failures and Their Effects

Such critical approaches are important for highlighting that biometric technologies are not neutral and objective but value-laden. At the same time, social scientific claims about the selective failure of biometrics are predominantly based on an analysis of technical-scientific literature on the performance of biometric systems in laboratory conditions. The consequence of this is that we need to be aware that the effects of certain calibrations (e.g. higher error rates for specific parts of a population) emerge within the context of experiments in a research lab, rather than in real-world applications, and that such effects cannot be assigned direct and straightforward societal impacts. Magnet therefore can be said to take big jumps in her line of reasoning when she writes that: '[…] biometric technologies that rely upon erroneous assumptions about the biological nature of race, gender, and sexuality produce unbiometrifiable bodies, resulting in individuals who are denied their basic human rights to mobility, employment, food, and housing' (2011, p. 51).

In their excellent analysis of the politics of Facial Recognition Systems, Introna & Wood (2004), after having scrutinized the algorithms and databases, conclude that there may be 'digital biases' (p. 192), but that it is crucial to understand how these become incorporated in actual practices of biometric recognition. Social scientific empirical studies on the use of biometric systems in practice, however, are scarce. The lack of such empirical studies may be explained by difficulties of access, as these systems are often used in sensitive contexts such as security, border control, or asylum management. A few recent (ethnographically inspired) studies on the roll-out of India's national biometrics-based ID programme (see Rao & Greenleaf 2013; Jacobsen 2012) discuss problems to enrol women and manual labourers, thereby highlighting the potential exclusionary effects of specific biometric technologies.

Yet they do not discuss operational details of the systems in the sense that they engage in what Introna (2005) terms a 'disclosive analysis' of the capturing technologies, algorithms, and databases that make up this particular biometric system. In general, it can be argued that despite such efforts to scrutinize biometric technologies, the design and functioning of specific technologies to some extent still remains a black-box.

Translation and Tinkering in Biometric Recognition Practices

In the remainder of this article we seek to expand on critiques regarding biometrics fallibility (Magnet 2011) and interpretations of this fallibility in terms of gender, ethnicity and racial bias, but also takes issue with some of these claims where they seem to rely on essentialist and deterministic argumentations. Rather than assuming that there is a pre-existing body or identity that biased technologies fail to read, and that biometric technologies almost automatically reinforce existing inequalities through their selective failure, we propose to analyse the multiple and complex ways in which bodily differences *emerge* during the design and use of biometric systems. This allows us to go beyond a general assessment in terms of a hidden dominance of whiteness, and to recognize the various ways in which system engineers and operators may know about and actively try to cope with the problem of bodily differences.

We first analyse how system engineers problematize the unequal distribution of errors among users of biometrics systems, and whether and how human bodily differences come up in particular translations of these performance problems. We use the concept of translation (a.o. Callon 1984) here to refer to the series of reformulations of a problem (the nature of which may be technical, social, organizational or other originally), so that it becomes amenable to techno-scientific analysis in a laboratory. The key points are that this process of translation is always contingent (and could have been done differently), and always involves a trans*form*ation of the problem, thus changing the range of thinkable/possible solutions.

Next, we look at the role of the operators and their possibilities for 'tinkering' and 'work-arounds' when operating biometric systems in specific contexts

(Suchman, 1987; Mol et al 2010; Grommé 2015). This allows us to denote the situated actions required of practitioners and users to bridge the gap between the rationalized protocols assumed in the technology, and the situational contingencies related to bodily differences encountered in practice.

Taking a relational view on biometric technologies and human bodily differences, we build on studies that seek to understand how bodily differences are enacted in particular practices (Mol and Law 2004; Mol 2002; Van der Ploeg 2011; M'Charek 2013). As M'charek (2013, p. 421) claims about race, '[it] is not a singular object "out there" in nature, but a relational entity enacted "in here."' In other words, human bodies (and their differences) are done differently in different practices. Bodily differences thus appear in multiple ways in practices of biometric recognition. Below, we analyse how such differences are produced, used, problematized and made (ir)relevant during the research and design phases of biometric systems, and when such systems are used in biometric border control practices.

Bodily Differences as R&D Challenges: Translating Performance Problems

The fact that errors and uncertainty are inherent to the process of biometric recognition is a well-recognized, major challenge for the biometrics community. While the majority of studies focus on the way environmental factors such as illumination influence the performance of biometric systems, human bodily differences have also become a relevant issue.

Identifying and Classifying 'Problem User Groups'

The biometrics literature acknowledges that some users 'are performing poorly as they cause a disproportionate number of verification errors' (Yager and Dunstone 2010, p. 220). These users '*consistently* receive poor scores, outside of what would be expected from random variation' (Yager and Dunstone 2010, p. 220). In reference to this phenomenon, the 'biometric menagerie', also referred to as 'Doddington's zoo', was suggested as a classification system of how well subjects can be biometrically matched against themselves and against others.

In this system, four animal metaphors are used to classify different user groups in biometric systems: sheep, goats, lambs, and wolves, according to the 'matching behaviour' they exhibit, reflecting these animals' metaphorically attributed behaviour. 'Sheep' make up the majority of the population of a biometric system. They behave as desired and 'match well against themselves and poorly against others'. 'Goats', however, 'are subjects who are difficult to match', and hence contribute to the false reject rate. 'Lambs' are 'vulnerable to impersonation', which means other users relatively easily match with them, while 'Wolves are exceptionally successful at impersonation and prey upon lambs'; both lambs and wolves thereby contribute to the false accept rate (Yager and Dunstone 2010, p. 220).

With this problem definition in terms of users' matching behaviour, the biometric menagerie implies that there are 'inherent differences in the "recognisability" of different users' (Jain et al. 2011, p. 22). An increasing number of studies thus locate the potential causes of differential recognizability of users in their 'demographic' characteristics (see Abdurrahim et al 2017). In a recent article, two biometric experts examine how what they term 'certain intrinsic properties of the subject, such as their ethnicity, gender and eye colour' (Howard and Etter 2013, p. 627) influence the distribution of errors in iris recognition systems. They conclude that:

> Particularly, Asian and African American individuals with brown eyes have a distinct propensity for being incorrectly not identified by iris recognition systems. In terms of Doddington's original classification scheme, these groups of subjects have a higher proportion of goats compared to the overall population (Howard and Etter 2013, p. 631)

Another study of age, gender and ethnicity as factors affecting the performance of facial recognition algorithms concludes that:

> First, as in previous studies, younger adults are harder to recognize than older adults. […] The second finding is that males appear easier to recognize than females. […]. Finally, as in past studies, East-Asians are showing up as more easily recognized than are Caucasians in datasets with a majority of Caucasian subjects. (Beveridge et al 2009, p. 762).

Human bodily differences thus emerge as 'intrinsic properties' of a person that are recorded as 'user metadata', enabling the classification of subjects into categories of ethnicity, gender and age, which then become conceived as controllable variables to be studied. As a result, the abstract (and metaphorically speaking hardly innocent) class of goats in an iris recognition system now appears to consist of individuals with brown eyes and specific ethnicities.

What these approaches to explaining the distribution of errors have in common is that they implicitly assume that the performance problem is with the users and not with the biometric technologies (see also Murray 2007). At first sight this seems to support existing social scientific accounts of the biometrics literature that stress designers' 'unreflexivity' regarding the 'white calibration of biometric systems' (Pugliese 2010, p. 60). Yet, a closer look at recent biometrics literature suggests such earlier critiques may require some nuancing, because actually, algorithms *are* opened up for scrutiny in several ways.

Problematizing the Workings of Algorithms: Face Recognition and the 'Other-Race Effect'

'State-of-the-art face recognition algorithms, like humans, struggle with "other-race face" recognition,' is the remarkable conclusion of a recent study (Philips et al. 2011). Whereas in the biometric menagerie algorithms simply do not feature as potential sources of problems, here we find them struggling to perceive differences between faces, and, even more disturbing to the researchers, resembling humans in their inability to perceive subtle differences between people of 'other races' than 'their own' (Philips et al. 2011). The implication, that algorithms are thought of as having a race, can be understood from the researchers' hypothesis that 'the geographic origin of the algorithm (i.e. where it was developed) affects its accuracy in recognizing faces of different races' (Philips et al. 2011, p. 3). They compared algorithms developed in 'the West' with algorithms developed in 'East Asia,'[1] and concluded that 'the East-Asian algorithm was better on East-Asian face pairs and the Western algorithm was better on Caucasian faces' (Philips et al. 2011, p. 9).

Yet, while this study showed that the other-race effect was present, it did not investigate its underlying mechanisms, because the researchers had no access to the source codes, or to the training and test image databases with which the algorithms were developed. This shows that algorithms are an opaque technology (Introna 2005), not only for the general public, but, to some extent, even for the biometric experts' community itself. Other studies, however, did manage to scrutinize training sets. Klare et al (2012), for example, found a clear impact of the 'demographic distributions' ('race/ethnicity, gender and age') in the training set on the performance of the algorithms on different 'demographic cohorts'

Here, algorithms are no longer considered neutral technologies merely measuring the similarity between two images, but appear as technologies with particular geographical origins, and particular learning experiences, even 'exhibiting biases' (Klare et al. 2012, p. 1) as a result of selective training. Pugliese's claim that biometric capturing technologies (camera's, scanners) are 'calibrated to whiteness' can therefore be extended as well as nuanced: in addition to the capturing technologies, algorithms too are tuned in specific directions. This calibration, however, should not be seen *solely* in terms of whiteness. The example of the 'East Asian algorithm' shows that certain technologies may also become calibrated to other colours or ethnic backgrounds (see also Maguire 2012). In addition, algorithms may be tuned to a gender or age category, so rather than to whiteness per se, algorithms may display a range of tendencies.

Moreover, these tendencies are not fixed, as algorithms can be re-trained. Computer scientists even suggest the use of 'dynamic face matcher selection', where 'multiple face recognition systems, trained on different demographic cohorts, are available as a suite of systems for operators to select, based on the demographic information of a given query image' (Klare et al 2012, p. 13). This idea to *use* gender, age, and ethnicity as supporting information for identification or verification, or for improving biometric system performance is gaining ground in the biometrics community (De Marsico et al 2013), where such classifications are also referred to as 'ancillary information', or, if done automatically by the system, as 'soft biometrics' (Jain et al. 2004). A growing number of studies focuses on such soft biometrics, i.e. the use of algorithms to detect and classify people into pre-defined categories of age, gender and ethnicity.

On Translating Performance Problems

In biometrics R&D, bodily differences thus emerge in various and complex ways in relation to the issue of biometric system performance. In translating performance problems into workable challenges, biometric system engineers enact bodily differences in multiple ways. Treating them as intrinsic properties of biometric subjects allows researchers to classify these differences into constructed categories of gender and ethnicity, and analyse them as external factors influencing the accuracy of a biometric system. Human bodily differences also emerge as the demographic distributions in a training set, which are understood to become part of the experience of algorithms, thereby tuning algorithms in specific ways. In addition, in image acquisition, bodily differences may become image quality issues and emerge as 'eyelid occlusion' in iris images, or 'insufficient' minutiae in fingerprints. Yet, from a social and ethical perspective, the more worrisome appearance of human bodily differences may well be their use in soft biometrics to improve system accuracy, or to narrow search spaces in databases, because of the black-boxing of these highly sensitive, and essentially contestable categories this involves.

Another crucial point here is that the attribution of failures and errors to the technology, to users and their bodies, or the interaction between the two is more than a rhetorical act. It problematizes the differential performance of biometric systems in different ways, and thereby also suggests different approaches for solving the problem. Attributing failure to the system encourages searching for the roots of the unequal distribution of errors in the hardware and software of the system. This could include reflexivity on the built-in norms and values, or the ways in which the algorithms were trained. Attributing failure and errors to (intrinsic) characteristics of users, on the other hand, makes the technology a neutral tool. As a result, solutions may focus on teaching users how to present their body part. Although such attributions do not necessarily determine the location of the solution sought, they do predispose towards a particular problem definition and solving strategy.

A focus on biometrics R&D thus highlights various ways in which bodily differences are enacted in the lab, but it does not tell us much about what happens when the wide variety of human bodies in the real world encounters biometric systems, for example in border checking practices. It is only by studying biometric systems in operation that we can understand how built-in normative assumptions play out in particular contexts and how biometric system uncertainties and errors are handled in situated practices. When, how, and for whom do bodily differences become relevant? When do problems arise and how do system operators, users, and technicians try to solve these? In order to answer these questions we now turn to empirical examples from our previous fieldwork.

Fixing Failures and Dealing with Differences: Tinkering at the Biometric Border

As we will show in this section, encountering and trying to solve biometric system problems related to bodily differences is part of the daily work of those who operate biometric systems. We briefly describe a two examples of 'tinkering' and 'work-arounds' at the border. The first case involves an automated border passage programme at an Asian airport. In this programme, members pay a fee, and have their background checked, and their iris enrolled in a biometric system, in exchange for the entitlement to use the automated gates at the arrival and departure checkpoints. The second example features the use of fingerprinting in a system for registering and verifying asylum seekers in the Netherlands, operated by the Dutch Immigration and Nationalization Service (INS).

Producing a 'Quality Image': Tears, Dances, and Grease

We start our enquiry at the enrolment centre of the automated border passage programme at the Asian airport, where new members are enrolled each day:

> A Chinese-American woman proceeds to the booth for iris-scanning. The capturing device consists of a camera with an integrated digital mirror and a rectangular drawn on it. The woman must look into the mirror and move her head until the eye is mirrored within the rectangular. Voice messages in English help her to position her eye correctly. First the left eye: an employee views the scan result and tells her to open her eye wider. A new scan is made. Now the image quality is 88%: just 2% below the required 90%. She tries again, and now the image is approved. The right iris appears to be even more difficult. The image is rejected six times. 'Please look into the square', the automated female voice repeats. Over and over again, the woman tries to open her eye wider by using her fingers to pull her eyelids apart. Tears start to flow from her eye and the employee hands her a tissue. Finally, after several other attempts, the image is approved.

Thus, significant efforts and adaptations were involved in producing an image of sufficient quality.[2] The work involved in producing a good-enough image includes users forcing their eyelids apart to present their iris to the system in the required way. The scanner also requires users to not move, rotate or tilt the head and to focus in the camera. Two technicians of the programme recounted that there were far more failures to read the iris at the gates in the arrival hall than at departures, because after a flight people were often tired and had more problems to focus and adapt their eyes to the scanner. Another telling example of the work involved in making oneself available to iris scanning comes from a recently terminated iris biometrics fast border passage programme at Heathrow Airport in the UK. This system was jokingly referred to by travellers as requiring them to do the 'iris dance', shuffling back and forth in order to align themselves with the camera (Palmer and Hurrey 2012).

In the automated border passage programme, image quality issues quickly became an important operational problem, explicitly linked by the system operators to the ethnicity of their customers. As a solution, the quality threshold of the iris images captured at the gates was lowered to 70%. A back-office technician explained that this was done to increase convenience, especially for members 'with Chinese roots'. Lowering the threshold meant that for most people a simple look into the camera sufficed to produce an image of sufficient quality without extra efforts. Thus, the operators tinkered with the technical settings of the system: high quality images at enrolment allowed them to lower the standards for the images captured at the gates, because the better the primary templates, the easier the verification of the secondary live images against them.

The second example[3] takes us to a Dutch INS office, where two fingerprints from every asylum seeker are enrolled in the Basic Facility for Aliens, and checked against Eurodac.[4] These data are then incorporated into the residence permits of non-EU migrants, and subsequently used for verification at all official encounters. In order to attain the improved accuracy for which the system was installed, however, significant workarounds are sometimes needed:

> I: How about the lady with whom it went wrong?
>
> P: […] the system says 'no match' for her fingers […] Are we going to refuse that lady a residence permit, because the prints might not be hers? […] The lady was a Somali national, and although Somalis do that, she had not mutilated her fingerprints […], I checked her fingers myself. Then I took her prints and got a 40% result. I was like: what is this? […] if you clean your fingers, then the prints are worse, if they are greasy, you gain better prints. What are the oily spots on your skin? It is here [points to side of nose] and on your forehead. So, to get good prints we ask people to rub these spots […]. Yet, these techniques were not helpful. Finally, the project manager said, put her four fingers on the scanner and fold them a little around the table, then you have the right pressure. It was not easy, but we improved the fingerprint quality. We achieved 80%; that was good quality. (INS officer, city A)

What we see in this excerpt is that the accuracy of a biometric system is in fact something that takes a lot of effort and additional techniques to be *achieved*. When her fingerprints fail to give a match, an asylum seeking woman from Somalia is first suspected of perhaps trying to sabotage the verification process by mutilating her fingertips because she is Somali ('Somalis do that'). The specific risk indicator for that type of sabotage (having mutilated fingertips) is subsequently checked visually by the INS officer: ('I checked her fingers myself'). After satisfying himself this way that no fraud is attempted, the negative verdict of the system is not believed, and all effort goes into the production of a better fingerprint scan, with some extra rubbing and greasing techniques. The belief in the first assessment is so strong, that even if all this fails, the project manager is asked to step in, and help out to achieve a positive verification by applying yet another tinkering strategy.

The Twin Sides of Tinkering

Accuracy, speed, and security are not inherent characteristics of biometric systems: a lot of work is continually required to achieve these outcomes in actual operational settings. This work includes ways in which operators, managers, and users understand and deal with errors and uncertainties and their interactions with human bodily differences. The example of the automated border passage programme shows that what constitutes an image of sufficient quality is by no means fixed. The image quality settings of the system became problematic in relation to users' bodily characteristics, but also to the aim of the programme, which was to deliver a fast and privileged border passage to paying members. Users adapted by pulling their eyelids, and operators tinkered by adjusting the required image quality, thereby overcoming the potential exclusionary effects of certain calibrations.

The other side of tinkering, however, is that it may introduce new uncertainties. Tinkering with the required threshold to produce a match or the required quality of the sample image in a biometric system may fix some failures, but also influences the amount and type of errors a system produces. The consequence of adjustable thresholds is that the security a biometric system produces is variable. Biometrics are often claimed to enhance both the speed and security of border crossing, but in operational contexts the setting of the threshold may more often be a trade-off between security (high threshold) and convenience and/or speed (low threshold). In the example of the automated border passage programme—which is a service programme with only a few thousand enrolled customers who have already undergone a background check at enrolment-, the required security level differs from that of other border control applications such as immigration control.

Tinkering may also introduce new risks. This becomes clear in the case of the female asylum seeker, whose identity claim of being at risk, that is, being a recognized refugee with a right of stay, is verified. Instead of the promised accuracy and certainty of digitalized biometric identity verification, a number of highly contingent factors determine whether she passes this verification test, including the assessment by the operator, the manager, the availability of the right levels of pressure and greasiness of the fingers to be scanned. For those whose fates depend on being believed, this introduces significant uncertainty and arbitrariness.

Conclusion: On the Politics of Biometric Systems

Critiques of biometric technologies are predominantly related to issues of surveillance, privacy and data protection, whereas the uncertainties and errors in biometric recognition practices have received far less attention. In recent social scientific studies, some of these biometric system problems have been interpreted as gendered and racialized calibrations and biases of biometric technologies. In this article, we departed from this work, but also called for a more nuanced understanding of the intersections between biometric technologies and human bodily differences. Rather than analysing how biometric technologies fail to read or represent (particular) bodies, we examined the multiple and complex ways in which bodily differences emerge during the design and use of biometric systems. In other words, we wanted to understand how bodily differences are enacted in biometric recognition practices.

Our analysis has demonstrated that while the software and hardware in biometric systems may have built-in norms about bodies and behaviour, these built-in tendencies should not be seen as having straightforward (in- and exclusionary) effects once the systems are used in practice. Technologies, including biometrics, do not produce effects by themselves, but only as part of particular practices that also comprise many other social and material elements (Van der Ploeg 2003). How certain calibrations, tendencies and technological scripts work out in practice thus also depends on other elements in the socio-material configuration that makes up a biometric system, including the environment in which it will be used and the tinkering practices of operators.

We also found that in biometrics R&D, bodily differences emerge in various and complex ways in relation to performance problems. While system engineers acknowledge there are differences in the performance of biometric systems on different users, they interpret the underlying mechanisms of these performance problems in multiple ways. The performance problem is sometimes attributed to certain intrinsic characteristics of the users, and sometimes to the hardware and software of the system.

This shows that in examining biometric errors it is not always possible to make clear distinctions between the effects of images databases, algorithms, system settings, and operators' practices. The relationships between biometric technologies, gender and ethnicity are emergent, multiple and complex. While this also entails that the political effects of biometric recognition practices are messier than is sometimes assumed, there are a number of issues that require attention.

First, even if the biometrics literature sometimes suggests that the differences in performance of biometric systems on different users are minor; an error rate of 0.1% seems almost perfect. When biometric technologies are used in high-stakes areas such as border control with millions of users, however, large numbers of people will be affected every day. Systems developed with limited test-sets cannot simply be transferred to (different) operational contexts. Moreover, in view of the increasing international mobility generally, and the dramatic refugee situation at Europe's borders today in particular, it is all the more crucial that any biometric system that becomes part of border management routines—such as the mandatory fingerprint verification of visa holders and registration of asylum seekers—works well with the widest possible range of people.

A second important issue is the attribution of error in biometric recognition processes. When too much trust or authority is put in a technology that inevitably produces errors and uncertainty, this clearly may have negative consequences for the people on whom it is used. When, for example, a non-match is routinely assumed to be a false identity claim by an imposter, this may lead to automatically putting the burden-of-proof on this person and, hence, to a violation of the presumption of innocence. Certainty and security are not inherent properties of biometric technologies, but rather the more or less contingent outcomes of chains of translations in specific checking practices.

Third, rather than biometrics' alleged failures to *represent* identity adequately, attention needs to be paid to biometrics' role in *producing* identity. Social scientists have argued that biometrics fail to adequately conceive of human subjects and identities (Magnet 2011), that 'human bodies are not biometrifiable' (Magnet 2011, p. 2-3) or warned that '[t]echnological systems no longer address persons as "whole persons" with a coherent, situated self and a biography, but rather make decisions on the bases of singular signs, such as a fingerprint' (Aas 2006, p. 155). From this viewpoint, biometric technologies *reduc*e identity to code, or the body to a password.

Yet, rather than assuming that there are pre-existing true bodies and true identities that biometrics fail to represent adequately or fully, biometric recognition practices may be better understood as ways to *establish* identity, in the sense that identity results from these efforts (Van der Ploeg 1999). This has the huge advantage of challenging us as social scientists to open-up these black-boxes and study all the contingent and perhaps contestable steps, translations, and decisions that go into these new ways of constituting identity. And, in view of current developments in soft biometrics, there is the more salient question: exactly which old or *new* definitions—and classifications of ethnicity, race or gender—will be enacted by these complex, opaque technological practices.

Notes

1. The researchers fused algorithms from China, Japan and South Korea to create an East Asian algorithm and algorithms from France, Germany and the US to create a Western algorithm
2. In the biometric literature, 'occlusion' (see for example Bowyer et al 2008), the partial covering of the iris by eyelids or eyelashes, is considered an important factor influencing iris image quality. It is only very occasionally, that a study mentions that this

occurs more often with 'Asian subjects' (see Liu-Jimenez 2009; Jillela & Ross 2013, p. 242).

3. With thanks to Karolina LaFors-Owczynik for conducting the interview from which the excerpt was taken. See also LaFors-Owczynik and Van der Ploeg (2016)
4. Eurodac is the main tool for the execution of the Dublin Convention (Council Regulation (EC) No 2725/2000) that determined that one cannot apply for asylum in more than one of the EU member states, and that the country of first application remains responsible for that person and their application (Van der Ploeg, 1999).

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by FP7 Security [grant number 608016], European Research Council [grant number 201853-2], and Universiteit van Amsterdam.

Notes on contributors

Sanneke Kloppenburg is a postdoctoral researcher at the Environmental Policy Group at Wageningen University. Her research focuses on the social implications of digital technologies in the context of energy and mobility. She is currently involved in two research projects about social practices and smart energy technologies in urban households. She received her PhD from the University of Amsterdam. In her PhD research she examined the regulation of international mobilities of people and goods at airports. Sanneke's work has appeared in journals such as *Mobilities, Journal of Economic and Social Geography*.

Irma van der Ploeg holds a degree in philosophy from the University of Groningen and received her PhD from Maastricht University. She has published extensively on philosophical, normative, social, and ethical aspects of medical technologies and ICTs.

References

Aas, K. F. (2006) 'The body does not lie': Identity, risk and trust in technoculture, *Crime, Media, Culture*, 2(2), pp. 143–158.

Abdurrahim, S. H., Samad, S. A. and Huddin, A. B. (2017) Review on the effects of age, gender, and race demographics on automatic face recognition, *The Visual Computer*. doi:10.1007/s00371-017-1428-z

Akrich, M. (1992) The de-scription of technical objects, in: W. Bijker and J. Law (Eds) *Shaping Technology/Building Society. Studies in Sociotechnical Change*, pp. 205–224 (Cambridge: MIT Press).

Amoore, L. (2006) Biometric borders: Governing mobilities in the war on terror, *Political Geography*, 25(3), pp. 336–351.

Beveridge, J. R., Givens, G. H., Phillips, P. J. and Draper, B. A. (2009) Factors that influence algorithm performance in the face recognition grand challenge, *Computer Vision and Image Understanding*, 113(6), pp. 750–762.

Bowyer, K. W., Hollingsworth, K. and Flynn, P. J. (2008) Image understanding for iris biometrics: A survey, *Computer Vision and Image Understanding*, 110(2), pp. 281–307.

Breckenridge, K. (2005) The biometric state: The promise and peril of digital government in the new South Africa, *Journal of Southern African Studies*, 31(2), pp. 267–282.

Callon, M. (1984) Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay, *The Sociological Review*, 32(1_suppl), pp. 196–233.

De Marsico, M., Nappi, M., Riccio, D. and Wechsler, H. (2013) Demographics versus biometric automatic interoperability, in: *International Conference on Image Analysis and Processing*, pp. 472–481 (Berlin: Springer).

Gelb, A. and Clark, J. (2013) Identification for development: The biometrics revolution. *CGD Working Paper* 315 (Washington DC: Center for Global Development).

Grommé, F. (2015) Turning aggression into an object of intervention: Tinkering in a Crime Control Pilot Study, *Science as Culture* 24(2), pp. 227–247.

Howard, J. J. and Etter, D. (2013) The effect of ethnicity, gender, eye color and wavelength on the biometric menagerie, 2013 IEEE International Conference on Technologies for Homeland Security (HST), IEEE.

Introna, L. (2005) Disclosive ethics and information technology: Disclosing facial recognition systems, *Ethics and Information Technology*, 7(2), pp. 75–86.

Introna, L. and Nissenbaum, H. (2010) *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, (New York: Center for Catastrophe Preparedness and Response, New York University).

Introna, L. and Wood, D. (2004) Picturing algorithmic surveillance: The politics of facial recognition systems, *Surveillance & Society*, 2(2/3), pp. 177–198.

Jacobsen, E. K. U. (2012) Unique Identification: Inclusion and Surveillance in the Indian biometric assemblage, *Security Dialogue*, 43(5), pp. 457–474.

Jain, A. K., Dass, S. C. and Nandakumar, K. (2004) Soft biometric traits for personal recognition systems, in *Biometric authentication*, pp. 731–738 (Berlin Heidelberg: Springer).

Jain, A. K., Ross, A. A. and Nandakumar, K. (2011) *Introduction to Biometrics*, (New York: Springer).

Jillela, R. and Ross, A. A. (2013) Methods for iris segmentation, in *Handbook of Iris Recognition*, (London: Springer).

Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V. and Jain, A. K. (2012) Face recognition performance: Role of demographic information, *IEEE Transactions on Information Forensics and Security*, 7(6), pp. 1789–1801.

Kloppenburg, S. (2013) Mapping the contours of mobilities regimes. Air travel and drug smuggling between the Caribbean and the Netherlands, *Mobilities*, 8(1), pp. 52–69.

LaFors-Owczinyk, K. and Van der Ploeg, I. (2016) Migrants at/as risk: Identity Verification and risk-assessment technologies in the Netherlands, in: I. Van der Ploeg and J. Pridmore (Eds) *Digitizing Identities. Doing Identity in a Networked World*, pp. 261–281 (New York: Routledge).

Latour, B. (1991) Technology is society made durable, in: J. Law (ed) *A Sociology of Monsters: Essays on Power, Technology and Domination*, (London: Routledge), pp. 103–131.

Liu Jimenez, J. (2009) Hardware/Software architectures for Iris biometrics, *Doctoral dissertation*, Universidad Carlos III de Madrid, 2009.

Lyon, D. (2008) Biometrics, identification and surveillance, *Bioethics*, 22(9), pp. 499–508.

Magnet, S. (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*, (Durham: Duke University Press).

Maguire, M. (2012) Biopower, racialization and new security technology, *Social Identities: Journal for the Study of Race, Nation and Culture*, 18(5), pp. 593–607.

Martin, A. K. and Whitley, E. A. (2013) Fixing identity? Biometrics and the tensions of material practices, *Media, Culture & Society* 35(1), pp. 52–60.

M'charek, A. (2013) Beyond fact or fiction: On the materiality of race in practice, *Cultural Anthropology*, 28(3), pp. 420–442.

Mol, A. (2002) *The Body Multiple: Ontology in Medical Practice*, (Durham: Duke University Press).

Mol, A., Moser, I. and Pols, J. (2010) *Care in Practice: On Tinkering in Clinics, Homes and Farms*, (Bielefeld: Transcript Verlag).

Mol, A. and Law, J. (2004) Embodied action, enacted bodies: The example of hypoglycaemia, *Body & Society* 10(2–3), pp. 43–62.

Muller, B. J. (2013) Borders, bodies and biometrics. Towards identity management, in: E. Zureik and M. Salter (eds) *Global Surveillance and Policing*, pp. 83–96. (New York: Routledge).

Murray, H. (2007) Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology, *The Communication Review*, 10(4), pp. 347–365.

Palmer, A. J. and Hurrey, C. (2012) Ten reasons why IRIS needed 20:20 foresight: Some lessons for introducing biometric border control systems, Paper presented at the European Intelligence and Security Informatics Conference (EISIC).

Pato, J. N. and Millet, L. I. (2010) *Biometric Recognition: Challenges and Opportunities*, (Washington: National Academy of Sciences).

Phillips, P.J., Jiang, F., Narvekar, A., Ayyad, J. and O'Toole, A.J. (2011) An other-race effect for face recognition algorithms, *ACM Transactions on Applied Perception* (TAP), 8(2), p. 14.

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

Rao, U. and Greenleaf, G. (2013) Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance, *Surveillance and Society*, 11(3), pp. 287–300.

Suchman, L. (1987) *Plans and Situated Action: The Problem of Human-Machine Communication*, (Cambridge: Cambridge University Press).

Van der Ploeg, I. (1999) Eurodac and the Illegal Body. The politics of biometric identity, *Ethics and Information Technology*, 1(4), pp. 295–302.

Van der Ploeg, I. (2003) Biometrics and the body as information: normative issues in the socio-technical coding of the body, in: D. Lyon (ed) *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*, pp. 57–73 (New York: Routledge).

Van der Ploeg, I. (2011) Normative assumptions in biometrics: On bodily differences and automated classifications, in: S. van der Van der Hoff and M.M. Groothuis (eds) *Innovating Government - Normative, Policy and Technological Dimensions of Modern Government*, pp. 29–40 (The Hague: T.M.C. Asser Press/Springer).

Van der Ploeg, I. and Pridmore, J. (eds) (2016) *Digitizing Identities: Doing Identity in a Networked World*, (New York: Routledge).

Van der Ploeg, I. and Sprenkels, I. (2011) Migration and the machine-readable body: Identification and biometrics, in: H. Dijstelbloem and A. Meijer (eds) *Migration and the New Technological Borders of Europe*, pp. 68–105 (London: Pallgrave MacMillan).

Yager, N. and Dunstone, T. (2010) The biometric menagerie, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(2), pp. 220–230.