University of Twente, Enschede, the Netherlands
Academic Year 2018-19

Faculty of Behavioural, Management and Social Sciences
MSc Philosophy of Science, Technology and Society - PSTS

Biometrics and Personal Identity: an alternative philosophical approach to the mainstream debate

FINAL PROJECT

Author: Simone Casiraghi
Student Number: 1859838
Word count: 19999

Supervisor: Dr. Kevin Macnish
Second Reader: Dr. Michael Nagenborg
Date of Submission: September 18th, 2018

Abstract

This thesis is about the ethics of biometrics technologies. In recent years, biometrics authentication technologies have been proposed as a solution for more efficient, secure and objective identification practices. My aim is to show how a philosophical analysis of biometrics under the lens of theories of personal identity could add new nuances to the mainstream debate. In particular, I have focused on so-called first generation biometrics (e.g. fingerprints, facial recognition, retina scans) for contemporary practices of identity management (such as current EU projects for border control and India's *Aadhaar* program). Accordingly, the main research question is: to what extent the study of biometrics technologies through the philosophy of personal identity could offer new perspectives to the existing ethical debate?

In the last decades, a new generation of sociologists and surveillance scholars (SSC) have put the topic of identity at the centre stage of the ethics of biometrics, arguing how such technologies, especially in EU practices of migration control, 'reduce' our dynamic and biographical identity to static biological samples. In this sense, biometrics are mainly seen as 'technologies of power', which enable institutions to 'control' citizens and 'exploit' their bodies; a dark side behind the promise of more efficient and objective identification practices.

In this work, I challenge and unpack both SSC's view and that of the biometrics supporters, and show how a thorough investigation of personal identity and the institutional embeddedness of biometrics could 'bridge' the gap between these two positions. Making citizens 'readable' not only gives the state a Panopticon-like power to constantly keep track of them, but also give persons a ground to claim for their rights. Still, some ethical problems could still arise (like asymmetry of access or epistemological loopholes), but they can be seen under a different lens from that of SSC. Biometrics for identification, however imperfect may be, could be morally justified providing that they are used in a responsible and more conscious way.

The structure of the thesis will be the following. In the first chapter, I look into the history of biometrics and identity management practices in general, to show the underlying idea that is (implicitly) purported by biometrics supporters. In the second chapter, I present the position of SSC and their main arguments against the use of biometrics. Finally, in chapter 3, I criticize SSC by offering an alternative theory of personal identity, and by identifying different epistemological and ethical concerns from the ones SSC focus on.

Table of contents

Acknowledgments

I wish to thank various people that contributed to this final project. First, I am particularly grateful to Dr. Kevin Macnish, my first supervisor, who enthusiastically guided and encouraged me throughout the whole process. His valuable feedback and inputs were key to the success of this project, and our discussions (in person and at a distance) gave me extra motivation and curiosity. The assistance provided by Dr. Michael Nagenborg, my second reader, was also greatly appreciated. His sharp observations and suggestions in the very early and last phase of writing certainly enhanced the quality of my work.

I wish to acknowledge the help provided by the team of Eticas Research and Consulting, where I spent three months as an intern, and I had the opportunity to actively work on European projects on biometrics. This experience enriched my theoretical knowledge and gave me new insights into the current uses of these technologies for border control.

Finally, a special thanks goes to my parents and to my girlfriend Anna-Carolina, for their important support throughout my study.

Introduction

The measurement of bodily and behavioural features can be seen as a powerful means to assess and authenticate one's identity. Today, biometrics technologies, which are becoming 'smarter' and digitalized, are often advertised as solutions both for the private and public sectors to increase security and efficiency in different areas such as airport security, border and immigration control, health systems and payment; at the same time, they have been raising ethical concerns, mainly related to privacy and discrimination.

In the current literature, there seems to be a gap between biometrics and identity as described by engineers and computer scientists (roughly, biometrics supporters) and by a new generation of social scientists and surveillance scholars (SSC), who sharply criticize these technologies mainly in the context of border control. My aim is to try to bridge this gap with a philosophical analysis, by offering a critical perspective on biometrics but without suggesting that it is intrinsically morally problematic for our identity.

To do so, I will criticize both the positions of supporters and opponents of biometrics by unpacking the premises of their arguments. In particular, by broadening the analysis to the institutional embeddedness of identity management technologies, I will show how 1) on the one hand, biometrics supporters do not take into account enough the practical limitations and drawbacks of the technologies (such as epistemological loopholes); 2) on the other hand, SSC focus too much on certain practices and fail to see the 'bigger picture' of biometrics technologies, which could serve as 'technologies of the self', i.e. as bases to claim for one's own rights. Still, I will not argue that biometrics are ethically unproblematic. Rather, with the help of an 'anthropological approach' of personal identity (Schechtman, 2014), I will shift the focus of what could go wrong in these technologies from the (narrow) issue of migration control and discrimination of asylum seekers (SSC and EU focus) to broader administrative problems in the distribution of state services (the *Aadhaar* program in India, for instance).

Research question(s)

The main research question is: to what extent the study of biometrics technologies through the philosophy of personal identity could offer new perspectives to the existing ethical debate? To address this main question, the following sub-questions will be investigated.

1) How can we define biometrics? What is the logic behind their supporters? How can the history of identification practices shed light on current biometric applications?

2) How can we define identity? How do SSC criticize biometrics with regards to identity? What is their theoretical (and possibly practical) alternative?

3) How can SSC be criticized? Is there an alternative theory of identity that could be applied to biometrics? What are the different ethical and epistemological concerns resulting from adopting such view?

Value

By addressing these questions, the thesis will add different perspectives to the current debate on identity and biometrics, so far dominated by arguments that draw on the work of Irma van der Ploeg and her idea of 'bodily information' (1999), and David Lyon and his idea of 'social sorting' (2003). A different take on personal identity, as well as an analytic investigation of epistemological issues, could help to avoid a polarization of the discussion and challenge a 'negative' attitude towards biometrics. This work could inform, in turn, policy makers and engineers (especially at a European level) and make them more aware of their implicit arguments, as well as provide hints for new lines of research in the political philosophy of biometrics.

Methodology

To reach these goals, the methodology used will be literature review and philosophical-conceptual analysis drawing on different approaches from the field of humanities. First, the history of technology will provide the background for identity management practices and the (recent) development of biometrics. Second, the current academic literature of surveillance studies will be investigated to define the mainstream debate about the ethics of biometrics. Third, analytic philosophy (in particular metaphysics of identity and epistemology) will be used to criticize the position of SSC and to provide a new angle to the current debate.

When dealing with concrete applications of biometrics technologies for border management, the EU project ABC4EU (2014-18) and Origins (2016) will be addressed. To avoid a Eurocentric perspective and an excessive focus on migration control, also the *Aadhaar* Indian program will be used as an example of a disputed biometric identity management practice. This case will not aim to show how India is having success with the program, but more to present different applications of biometrics that could be potentially useful and yet deserve attention from a different perspective.

Overview of the chapters

The thesis consists of three chapters. In the first, I will give a terminological and historical overview of biometrics and identity management. I will look into definitions and

characteristics of biometrics (first and second generation) and into how modern states have been trying to create reliable identification practices (also with the help of ID documents) to make citizens fulfil their duties or benefit certain services. With this framework, I will sketch the underlying narrative of biometrics supporters, with reference to some EU projects for migration control and to India's *Aadhaar* program.

In the second chapter, I will move to the mainstream critique of this narrative made by SSC. I will first philosophically investigate the concept of identity, and show how SSC focus on a qualitative (*who* am I?) rather than a quantitative (*what* am I?) account of identity. Then, I will characterize SSC's position as based on a critique of bodily criteria of identity (*we* are our bodies) and on certain foucaultian ideas of 'biopower' and surveillance. In line with this premises, SSC critique biometrics for 'reducing' the whole of our dynamic and biographical identities to our static biological samples. However, I will show how their theoretical alternative, based on an idea of narrativity (which recalls a psychological criterion of identity) and a 'borderless' society is not completely satisfying.

In the third chapter, I will challenge this view by introducing an 'anthropological criterion' of personal identity as a 'third way' to metaphysical and practical approaches to identity. In short, I will argue how identity is based on our social infrastructures and recognition practices as well as on metaphysical criteria (Schechtman, 2014). This view will show how actually biometrics do not reduce our personal narrative identity, but instead bring more narratives to the mix and possibly help people claim for their rights. Still, I will balance this more 'positive' take on biometrics by showing how a crucial ethical problem of biometrics is not that our identities are reduced, but to make sure that such reductions are kept to a minimum in the whole socio-technical infrastructure of identity management.

1. Biometrics technologies and identity management

1.1 Brief history of identification practices

Let me begin this chapter with a famous case from the past: the story of Martin Guerre in the 16th Century France (Cole, 2001, 6). Martin Guerre was a French farmer who disappeared from his village in 1548. Some years later, in 1557, another person (who would be later identified as Arnaud de Tilh) came to the village and passed himself off as Martin Guerre. The physical resemblance, as well as his detailed knowledge of Martin's past life, made Martin's family and villagers believe Arnaud's story. As a result, Arnaud started living as if he was Martin. After three years eventually, in the wake of the doubts and subsequent investigations of Martin's father, Arnaud was suspected as an impostor and processed. After several trials (to which the 'real' Martin Guerre, who meanwhile had returned to the village, assisted), he was found guilty and executed in 1560.

This case is particularly intriguing because it turned out really difficult to find consistent parameters or features to correctly identify Martin Guerre. Was the Martin Guerre that appeared in 1557 the same as the one who had disappeared in 1548? How was it possible to 'prove' that or the contrary? What were the consequences of failing to identify Martin as Martin? At the time, evidence relied mostly on the memories of the defendant and of the witnesses. Many villagers swore that Martin Guerre was taller, darker and with a scar on his eyebrow. Others, however, confirmed the accused was indeed Martin, as he had three warts on his hand and extra teeth (Cole, 2001, 6). Today, with the development of more sophisticated biometrics identification techniques, which rely on unique bodily traits, it seems that the case could have been solved earlier. Photographs, fingerprints, ID cards or a DNA test would have proven that Arnaud was an impostor. However, it would be too shallow to think of technologies as 'fixes' with no drawbacks for our societal problems. As it has already been shown (Meijers, 2009), the development of new technologies, and the practices associated with them, could bring about new ethical problems. Before finding out whether and to what extent this is the case, it is useful to step back and investigate more such technologies and practices themselves.

Accordingly, this chapter will introduce the reader to biometrics technologies for the purpose of identity management. With "identity management" systems I refer generally to "ways and methods of dealing with registration and authorization issues regarding persons in organizational and service-oriented domains" (Manders-Huits, 2010, 43). More intuitively, an identification practice is an action to attribute 'identity' to an item (Mordini & Tzovaras,

2012, 1). For now, I will use the following working definition of identity: "identity can be seen as the state of being the same (or identical) of persons and things" (I will say more on this in chapter 3).

The Western philosophical tradition has been struggling to find a solution to the puzzle of the criteria of identity of an object throughout time. The whole ancient Greek tradition, for instance, can be analysed through the lens of the different solutions given to explain the unity in the plurality of things (Plato's forms and Aristotle's categories for instance) or, in other words, how something remains the same and persist throughout time despite changing (Heraclitus' paradox of the ever-changing river vs. Parmenides' *One*).

In this work however, in line with the 'empirical turn' in the philosophy of technology (Achterhuis, 2001) and differently from most of the philosophical tradition on the topic, I do not want to start from metaphysical issues to then, eventually, inform or explain how we practically deal with identity issues. On the contrary, I want to start from concrete identity practices (and the technologies involved in them) to then, in turn, inform and reflect on the metaphysics and ethics of personal identity. The reason for my choice is that a traditional approach could lead to too abstract consequences (e.g. that the concept of identity is useless or non-sense), thus preventing experts from different fields (other than philosophy) to find a 'common ground' to start an interdisciplinary debate on biometrics.

To do so, it is worth mentioning that, historically, it could be argued that methods for identification almost stem from a human need, which can be traced back (even with some controversies) *at least* to the birth of the first urban societies in the Neolithic Revolution (Mordini & Tzovaras, 2012, 2). To simplify, the transition from a hunter-gatherer economy to an economy based on farming and agriculture contributed to the emergence of sedentary dwelling. Such economy also created more and more food surpluses and thus the possibility of trading them with other nearby populations. Along with a growing societal complexity and trading systems, the identification of 'the stranger' became of vital importance for the functioning of these early societies. In fact, with the creation of more and more 'fixed' physical boundaries of villages and communities, the recognition of 'unknown' people (who were not part of such community and therefore could be potential threats) became crucial for the sake of social order and conflict avoidance (Mordini & Tzovaras, 2012, 2). Still, practices of identification were mostly dependent on local settings (Lyon, 2009, 45). Identifiers in early societies could include physical traits (like body size, hair colour, particular scars or deformities) as well as permanent body modifications like tattoos. Moreover, tokens (like rings, a pass or a seal) and mental contents (as memories, music, poems) were important

identifiers. Archaeologists found 75000 years old shell beads is South Africa, which could suggest that people used jewellery for identity purposes (both recognition of the other and self-awareness) even long before the Neolithic Revolution (Malafouris, 2008).

With the birth of the great empires of the past (e.g. Egyptian, Assyrian and Chinese), issues of taxation, conscription and execution of the law pushed forward the need of more accurate identification systems. It is for these purposes, for instance, that under the Roman Empire a tripartite codified name scheme was introduced (Mordini, 2014, 508). Similarly, the assignment of individual last names (as opposed to patronymics, suited for smaller communities) in China at least since the 2nd Century BC (Koon, 2016) and in Europe in the Middle Ages was part of a project of legibility of the state to ensure that its inhabitants could function as citizens and as legal persons (Behrensen, 2017, 62).

With the modern era, and the birth of national states in Europe, the need for even more effective recognition schemes was required by the increasing mobility, urbanization and (later) industrialization of this period, as well as by the growing relevance of state borders (Mordini & Tzovaras, 2012, 3). This period saw a transition from community or local-based to national and centralized identification practices. In other words, each state, to function properly, needed to record and manage information about individuals without the necessity to rely just on local knowledge (like the eye-witnesses in Martin Guerre's case). Certificating and acknowledging citizens' identities was realized by the establishment of an 'identity chain', which starts with birth registration and ends with a death certificate (Mordini & Tzovaras, 2012, 4).

More recently, after World War II many countries introduced national systems of identity cards including facial photography and sometimes fingerprints (Mordini, 2014, 509). A major drive to this transition can be considered the need to identify people entitled to receive social benefits. In fact, the welfare state, first appeared in Northern Europe and based on the equal provision of social and economic well-being by the government, needed, among other things, reliable identification practices, like social cards or social insurance numbers issued by the state (Lyon, 2009, 45).

Today, in a global and interconnected world, new issues that transcend traditional identification schemes and require new solutions are emerging. As Mordini (2014) puts it, "The tourist hoping to use her credit card in any part of the globe, the asylum seeker hoping to access social benefits in her host country, and the banker hoping to move money from one stock market to another in real time – all have the same need. They must prove their identities and be certain of others' on a global level" (509).

1.2 Biometrics: definitions and conceptual clarifications

It is in this context and for these purposes that biometrics have been proposed as a possible solution to effectively identify people. Before exploring possible advantages of biometrics systems, it is necessary to open a parenthesis about the very same definition of 'biometrics'.

In spite of the growing literature in recent years, the definition of 'biometrics' is still debated. Mordini & Petrini (2007) delineate the history of the word, which originates from the Greek words *bios* (life) and *metron* (measure) (6). By analysing different dictionary definitions, the authors trace the origins of the discipline back to the 17th Century, as a part of the theoretical project, initiated by Galileo, "of measuring all that could be measured and make measurable what cannot be immediately measured" (Mordini & Petrini, 2007, 6).

Nevertheless, the use of the term as indicating a unified field of scientific inquiry has become common, in the English literature, only from the early 1980's (Wayman, 2007, 263). The spectrum of what is usually referred to as 'biometrics' is in fact wide and includes disciplines from distinct scientific traditions. Hence some experts build their definition focusing on the types of trait or information that are collected (e.g. fingerprints, facial image), others on the types of technology employed (e.g. CCTV, body-scans) and others on their application (e.g. migration control or e-commerce).

To clarify, I will elaborate on two definitions to come up, eventually, with a narrow working definition. The reasons why I chose these two are that: (1) they are well representative of the literature on biometrics; (2) they contain general characteristics of biometrics instead of specific applications or technologies; (3) they are made by a group of scholars (SSC) I am going to confront in the next two chapters [1]. First, Ajana (2010) describes biometrics as "the technology of *measuring*, analysing and processing the digital representations of *unique biological* data and *behavioural* traits such as fingerprints, eye retinas, irises, voice and facial patterns, body odours, hand geometry, etc." (238, italics added). Similarly, Ceyhan (2008) interprets it as "the *automated* use of physiological, biological, genetic or behavioural features to assess the *uniqueness* of the person and to *verify* and *authenticate* his/her identity" (113, italics added).

I believe that two main characteristics emerge from these (similar) definitions.

1) Firstly, there is an issue of measurability (*metron*) (Mordini & Tzovaras, 2012, 7). In fact, biometrics target not just general physical properties but specifically measurable physical properties. Today, to identify someone, the technology works, approximately, in the following way. Automated identification machines link the output of a biometric machine

reader (say, a fingerprint reader) to an existing archive of records via an algorithm. To obtain such archive, beforehand, a 'sensoring' device collects data from the individual. Samples can be collected from many bodily traits, both biological and behavioural, depending on the data one aims to collect (see point 2 below). Then, the digital representation of the data is transformed via an algorithm to produce so-called 'templates', which are stored in centralised databases. Whenever, on subsequent occasions, such data are collected again, they can be automatically matched with existing templates and, if a matching is found, the person is 'recognized' by the system (Van der Ploeg, 2007, 46). To make it more concrete, think of when you unlock your smartphone with your fingerprint, like with the Touch ID system in iPhones. First, your fingerprint is 'saved' as a password in the system (in the case of iPhone, it asks you to lift and rest repeatedly your finger on the home button). Then, every time you want to unlock your screen, by placing your thumb on it, the system can 'recognize' your trait and allows you to access to your apps, photos and purchases. If no match is found, the screen remains in a locked mode.

Such standard procedure relates to another important aspect of contemporary biometrics that is mentioned in Ceyhan's definition, that is the 'automated' characteristic. Human-based biometrics identification practices have historically been employed for centuries [2]. However, what makes it urgent to analyse digitalised biometrics from a philosophical perspective is that such identification practices can be made i) entirely or partly by machines, thus by-passing human decision-making; ii) by using huge quantities of data that can be matched with a rapidity and accuracy unknown to the more 'traditional' human-based identity management practices (Mordini & Tzovaras, 2012, 7).

Potentially, according to biometrics supporters, there is no longer (or less than in the past) need for a human eye that matches the sample and its actual representation. In other words, 'digitalizing' biometrics would mean that the identifiers of a person are turned into digits and manipulated by algorithms through numbers.

Technically, such match between the collected data and the existing template is called 'identification' when it occurs with reference to a database (one-to-many) and 'verification' when it occurs with reference to one single template (one-to-one).

2) The second characteristic of the definitions is the link between biometrics, the human body and its visible biological or behavioural features (*bios*). Biometrics recognition, so it appears, is based on the assumption of two features of bodily traits: distinctiveness (or uniqueness) and permanence (Jain & Kumar, 2012, 50). In other words, it seems that living beings, and

humans in particular, have specific qualities that are unique (i.e. the same are unlikely to be found in two different individuals) and permanent (across time) enough to ensure a correct identification. Such biological or physiological traits that are measured can be indeed very different. However, engineers usually distinguish between *strong*, *weak* and *soft* biometrics features (Mordini & Tzovaras, 2012, 8).

Some traits are considered 'strong' because more permanent and unique than others, such as fingerprints, iris, retina or hand veins. Even though, to be fair, no qualities could be considered 100% unique or permanent, some patterns could be practically considered as such. The same holds, for instance, in the animal kingdom in the case of muzzle patterns of cattle or tiger stripes (Bromba, 2007). 'Weak' biometrics traits instead are considered less unique and stable. In humans these are, for instance, body shape, odours, behaviour (including gestures, facial expressions and gait), voice, or electrophysiological phenomena like brain waves (Mordini & Tzovaras, 2012, 9). When used for identification, weak biometrics are usually combined with strong features. Lastly, 'soft' biometrics traits are more generic and cannot be associated with specific individuals, but nonetheless can contribute (in association with strong and weak features) to identify an individual. Examples include categories like gender, age, ethnicity, height, eye colour, etc.

Another common distinction found in the literature is between first and second-generation biometrics, or between traditional and more futuristic technologies. As a rule of thumb, early applications of biometrics, like fingerprint or facial image, fall under the first category. Conversely, second generation biometrics require less human cooperation and can be run in a transparent and 'invisible' way to the subjects. This has led to a shift from human eye performed identification (e.g. traditional fingerprint analysis) to increasingly automated, digital and 'smart' biometrics. Examples are technologies that measure 'motor skills', electromagnetic body signals or human-computer interaction patterns (Mordini & Tzovaras, 2012, 9). Moreover, the combination with big data and ICT could create integrated systems of multiple biometrics systems used at once. Therefore, second generation biometrics are able to capture more characteristics of an individual. Not only are they based on morphology (e.g. fingerprints, passport photo) but on physiology and behaviour as well. Gestures and behaviour could provide information on cultural features, while face or brain waves on mental activities and emotions.

Despite the great interest they raise, the use of second generation biometrics is often still speculative and their technological development in its early phases. Moreover, the distinction

between the two groups can be debated because it is difficult to trace a clear cut line: on the one hand, some biometrics are used in combination with one another (e.g. is facial recognition 'only' a first generation biometrics if used in combination with technologies that track facial expressions?); on the other hand, the very same distinction between purely physiological-behavioural and biological-genetic features can be challenged (think of the complex nature-nurture debate for example) [3]. However, it is not my purpose here to dwell further on the problems of the definitions of biometrics. This excursus was necessary to create a background and explain what is at stake when we refer to biometrics, and merging the two working definitions above (those of Ajana and Ceyhan) suffices to support my argument. Accordingly, we could define biometrics as "the automated technology of measuring, analysing and processing the digital representations of unique biological data and behavioural traits to assess the uniqueness of the person and to verify and authenticate his/her identity".

Having said that, to narrow down the field, and in accordance with the labels of the current debate, the thesis will mainly focus on first generation biometrics. From now on, only the term 'biometrics' will be used to make the reading smoother.

1.3 Biometrics and borders: security and efficiency enhancement

Now that the definition of biometrics is clearer, it is possible to go back to the idea of biometrics as a solution to identity management issues. As we are living in the so-called 'Information Age' (Castells, 1999), identification has become even more important than in the 'traditional' paper-based bureaucracy (Lyon, 2008, 500). As Lyon (2008) notes, nowadays "[t]he employee authenticates her identity with an access card to enter the workplace, the traveller shows a passport to board a plane, and the patient produces a health card to prove eligibility for medical services at the hospital. Without the card, and the databases on which it depends, identity cannot now be verified. Telling your story no longer suffices. It is displaying your card that counts" (500). In general, biometrics are already in use in many existing (and proposed) national ID card systems or travel documents (Lyon, 2008, 500).

Such applications are used to control movement and access, but also to reinforce security. In this regard, one particular application of biometrics I want to focus on is border security [4]. In recent years in the US, after 9/11 terrorist attacks, upgrades in the identification systems in the name of national security have been put on top of the list. Particularly, since airports played a key role in major terrorist attacks, biometric identification has attracted attention and is being increasingly used to enhance aviation security (Murphy & Maguire, 2015). For instance, foreigners from 28 countries entering US airports and seaports have to provide their

fingerprints and photographs upon entering the country (Robertson, 2009, 348). Similarly in Europe, after terrorist attacks such as those in Paris (2015), anti-terrorism and security [5] efforts have become extremely important on the agenda of the European Union (Bigo, 2014; Ceyhan, 2008; Redpath, 2007). In parallel, also in relation with the war in Syria (FRONTEX, 2014), the crisis of migration management has become more urgent, especially for those EU member states that are closer to non-member states, like Italy, Spain and Greece (Pappas, 2016). In contrast to the past, migration is today often felt as a 'threat' that calls for protection and restrictive policies (Pécoud & de Guchteneire, 2006, 70).

But how can biometrics be a solution for identification problems in this field? As shown in § 1.2, supporters of biometrics find such technology attractive as it can achieve identification by using features that (almost) all humans have, in a relative quick, non-invasive and low-risk procedure (Lyon, 2008, 501). In fact, speed and security issues are reconciled: increasing the speed while processing travellers can have a positive impact on security. This is the idea behind crowd management practices: large groups of people need to be controlled to avoid disorders. If long lines of travellers are left unprocessed at an airport because of the inefficiency of identification practices (e.g. not enough border guards per number of travellers), there is a security risk (Murphy & Maguire, 2015, 165).

Specifically, digital biometrics can be faster and more secure because more 'objective' than traditional identification practices. This idea of objectivity comes also from the field of forensics, where fingerprints were massively employed until the 1970s to identify criminals (Mordini, 2014). Today, there is a similar case in forensics with DNA, which has a sort of 'magical aura' of infallibility and it is often referred to as a 'silver bullet' or 'golden standard' for identification (Dahl, 2009, 219). I believe that, in the context of migration, the label 'objective' can be actually intended in two distinct senses, one *epistemological* and one *moral*.

1) First, in an epistemological sense, biometrics are considered a scientifically *sound* form of identification. As already noted above, especially for 'strong' biometrics some traits are considered particularly unique and permanent. As already noted, automated systems of biometrics identification are seen to outperform the current limitations of human-driven verification systems. In this sense, for instance, biometrics systems would be more 'reliable' and efficient in identifying potential terrorists or illegal migrants who try to cross the borders.

2) Second, in a moral sense, biometrics are an *impartial* form of identification. The process of recognition is carried out by *automated* systems, thus boosting the fairness of the outcomes. The idea is that, while people can have biases, automated machines do not, and are consequently more equitable (for a criticism of this point see Macnish, 2012).

In sum, the body, along with its biometrical features, is frequently seen as secure and useful to protect identities and personal information. This is why some authors have argued that biometrics supporters see the body as a password. As Aas (2006) explains it, "not only does the body not lie. It also tells the truth, and it is an encoded truth which, like numbers, computer passwords and PIN codes, is objective and unambiguous" (153).

These two characteristics, i.e. soundness and impartiality, it is argued, could enhance security and diminish discriminatory practices. For instance, airport security could be upgraded by making more accurate and efficient controls at check-ins, in order to cut down risks of terrorist attacks (Aas et al., 2009, 1-17). Moreover, in terms of securing one's individual identity, the objectivity of biometrics profiles could enhance privacy by, say, reducing identity theft (Thomas, 2005).

More interestingly, advocates claim that automating identity checks could potentially *reduce* discrimination. The use of 'objective' profiling technologies could reinforce confidence in border security and migration control operators, reducing the myths and stereotypes associated with migrants and asylum seekers (Thomas, 2005).

1.4 Case studies: European Projects and India

To show how governments and institutions are more or less implicitly supporting this narrative I want to focus on two case studies in particular: current EU projects and India. In these cases, modern passports, where biometrics identifiers are stored, play a key role.

Differently from simple ID documents as described earlier in § 1.1, passports were created in Europe [6] to help nation states to control legitimate means of movement (Torpey, 2001, 256). Not only were they made to allow people to travel freely across countries (as a *laissez passer*), but also to prevent them to do so. Especially after World War I for instance, the denial of passports was used as a 'weapon' to deny untrustworthy citizens the possibility to leave their country (Behrensen, 2017, 73). However, it must be noted that the passport cannot be reduced to no more than a mechanism of state control (Torpey, 2000, 159). In fact, this document is also a means to *protect* its holder while in the jurisdiction of other states.

However, in recent years, the role of the passport as a mechanism of control over individual movement has become predominant (Torpey, 2000, 160). And such purpose, in line with the narrative described in § 1.3, can be enacted more efficiently thanks to the transition from non-biometric to biometric passports. The key of this transition is the introduction of a standardized [7] embedded microchip that stores the biometrics information of the document's holder (Heimo et al., 2012, 69).
The passport as a standardized identity document has a pivotal role in current European projects such as ABC4EU or ORIGINS, where the information contained in an e-passport, matched with biometrics parameters, could permit or prevent travellers to enter and exit the Schengen area. The ABC4EU project (2014-2018) (Automated Border Control Gates for the European Union) is a EU funded project whose aim is to make border control more flexible and efficient by enhancing the workflow and harmonizing the functions of the *e-gates* at air, land and sea border crossing points. Murphy & Maguire (2015) make it clear how such ABCs work by checking both traveller's fingerprints and facial image:

"In order to pass an ABC gate, each person must place their passport face-down on a document reader or slot their national ID card into a reader […] The facial data contained in one's passport is compared to live biometric data by means of a rapid-burst imaging using an adjustable camera that selects the best from a number of images taken. If a sufficient matching score is achieved then the traveller may proceed through the gate" (163).

However, EU initiatives are not just limited to the securitization of borders through the introduction of biometrics features in passports. Biometrics are also used to make the whole 'identity chain' more secure, as shown by the project 'ORIGINS' (2016). The project addresses the issue that so-called breeder documents, which are 'basic' documents used to obtain other identity, residence and travel documents (like passports or driving licences), are easy targets for fraud and identity theft. Examples of breeder documents are birth, marriage or death certificates, which are relatively easy to copy, since the requirements for their creation and verification are not always clear or harmonised across international borders. As a result, breeder documents are often referred to as the weakest link in the so-called "identity chain" that starts with the registration of one's birth and ends with the registration of one's death. To securitize these documents, in 2016 the ORIGINS project studied the technical viability and desirability of the introduction of biometrics features in breeder documents (such as fingerprints in birth certificates).

The efforts made by EU to implement biometrics systems in identification practices are not unique. An exemplar case outside Europe is that of India, that in 2010 launched its *Aadhaar* program (probably the world's largest biometrics system) to enrol biometric data (among which, iris scans) of all its citizens. The context and identity infrastructures of India are of course very different from those of the EU. According to Daugman (2014), the main purpose behind this project is not just security but entitlements distribution:

"Only one in 12 persons has a bank card. Only 4.2% have passports. Hundreds of millions have no official ID, and many have multiple IDs. Some States within India have many more names on their food ration lists than the number of persons who live there. Many subsidized commodities (such as kerosene) flood the black market because bogus benefits cards abound. Widespread fraud prevents fair distribution of entitlements" (1).

Issuing a 12 digit Aadhaar number to anyone who asks for it (the system is not mandatory yet) would help citizens to have a unified identification document that would capture all the information to assert their identity and benefit from government services.
Although the selection of these cases is the result of my personal choice and experience, the order whereby I listed them is not casual. While many European citizens could at first sight agree with the motivations of EU projects such as ABC4EU, the case of India seems to go too far. In particular, the latter case could immediately evoke a dystopian 'Big Brother'-like scenario. Nonetheless, are these two cases so far from one another? Are there any ethical problems that could rise from all these situations?

1.5 Some general criticisms

Many critics of biometrics have focused on particular ethical-legal issues of privacy and violations of human rights such as the protection of personal data, personal liberty, confidentiality, human dignity and the relations between individual and collective rights (Mordini & Petrini, 2007, 7).
For example, the RAND report (Woodward et al., 2001) identifies three areas of ethical and social concerns brought about by biometrics:
1) informational privacy;
2) physical privacy;
3) religious objections.

With (1) the report makes reference to (i) 'function creep' (i.e. the use of the technology beyond the purpose for which it was originally intended); (ii) 'tracking', i.e. the ability to monitor individuals' actions in real time; iii) data misuse, such as the possibility of identity theft (Woodward et al., 2001, 23). As for (2), the report mentions the possibility of harming the participants with the use of the technology; the case of stigma associated with the use of biometrics; and finally, the concerns that the devices used to 'read' bodily features could be unhygienic. Regarding (3), the report remarks how people could refuse to give their biometric data on the basis of their religious beliefs. As an example, some Christian groups in the US consider biometrics as an image of the Devil, on the basis of some interpretation of the Book of Revelation in the Bible (Woodward et al., 2001, 28).

These criticisms are certainly relevant for the public debate, but they go beyond the scope of this thesis. In fact, upon further scrutiny, in my opinion, they risk to frame the debate in a cost/benefits analysis (like the security vs. privacy debate). From a philosophical perspective, I find it more interesting to reflect on the very same (implicit) conception of personal identity held by biometrics supporters.

In particular, it could be argued that there is a problem of circularity in the security argument (Behrensen, 2014). Biometrics are used to establish an identity only to later be used as a proof of the identity they helped to establish (identity is assumed rather than proved). But what type and criteria of identity are then assumed? Why is the body so important to identify a person? Are our identities fixed and 'already there' or they are co-constructed through these identity management practices? Addressing these sub-questions will be the task of the next chapter.

Notes

[1] I will engage particularly with the works of Btihaj Ajana, Katja Franko Aas, Louise Amoore, Ayse Ceyhan, David Lyon and Irma van der Ploeg.

[2] The Portuguese historian João de Barros argues that the use of fingerprints dates back even to early Chinese merchants to settle transactions in the 14th Century (Garfinkel, 2000, 38).

[3] Intuitively, one could ask to what extent our behaviour is determined by biological traits, and to what extent our biological traits could also be modified by the environment.

[4] This choice is due to the fact that: (1) I personally worked on biometrics and border security for Eticas Research & Consulting on the ABC4EU project (see § 1.4); (2) it would not be possible to make concrete examples of all possible applications of biometrics in such a short thesis; (3) most of the current literature on the ethics of biometrics is focused on this field.

[5] In this context, 'human security' can certainly be a fuzzy term. To make it clearer, I will borrow the definition provided by Gasper (2009): "Human security means, in a broad formulation, the security of human persons, against important threats to their basic needs. It refers to the security of all people, not just the security of the security forces, or of the state, or of the rich" (4). Since the purpose of this work is not primarily security, this working definition suffices to build my argument.

[6] Passports thus conceived were first issued in France by Louis XIV, and linking the personal identities to birth registration was enacted during the French Revolution (Mordini & Tzovaras, 2012, 3).

[7] These standards are defined by the International Civil Aviation Orgainization (ICAO, 2015).

2. The criticisms of (some) surveillance scholars to biometrics

2.1 Introduction to SSC criticism

In order to provide a new philosophical angle to biometrics and its ethical implications, further inquiries into the notion of 'personal identity' are needed. In fact, in which ways is biometrics about the uniqueness of identity and what type of identity are biometrics supporters concerned with?

A new generation of sociologists, criminologists and surveillance scholars (SSC) has tried to unpack these questions and is particularly concerned with the use of biometrics for security purposes. Two major scholars inspire much of their work. First, the philosopher Irma van der Ploeg has drawn attention to the role of the body and how it is put "at the centre of the stage" in current identity management practices (1999; 2007; 2011; 2012). Secondly David Lyon, who recently turned surveillance into a major issue for social scientists, reads biometrics as a Foucaultian, 'panopticon-like' and 'biopolitical' practice [1] (Lyon, 2003). Both, in general, agree on the fact that the biological aspects of biometrics and their consequences for people's identities are the most problematic. The main observation these authors make is that the same biometrics features and identification technologies that are used can be indeed quite convenient and efficient for some, but they are also used to restrict the movement of others (Aas, 2011, 336; Ajana, 2010, 247; Amoore, 2006; Ceyhan, 2008, 113; van der Ploeg, 2012, 181). This would lead on the one hand to the reinforcement of privileges of some groups (like EU and US citizens) and on the other to the increased discrimination of other groups (like asylum seekers). Here is a significant quote by Aas (2011):

"[T]hese practices are predominantly directed at specific groups of 'crimmigrant' others who form a class of subcitizens, where crime control objectives define the terms of their exclusion from the bios. The flip side of this negative exceptionalism is the positive exceptionalism directed at *bona fide* foreign citizens who, although treated as potential crimmigrants in the vetting procedures, are nevertheless empowered by surveillance, to open gates that remain closed to the vast majority of the world's less privileged populations" (342).

To exemplify this point, think of these two cases. First, consider the FLUX traveller program for US and Dutch frequent intercontinental travellers, which is based on biometrics identifiers among which fingerprints and eye imaging (Aas, 2011). In brief, so-called 'low risk passengers', i.e. "with no criminal records, no customs or immigration conviction" can apply

for the program. If the interview and security threat assessment is successful, they can have, at a cost of paying an additional fee, the advantage of skipping queues and border checks [2] (Aas, 2011, 336).

By contrast, think of the EURODAC database, which stores the fingerprints of asylum seekers and irregular border-crossers who enter the EU and whose aim is to restrict the movement of this group of people. In the wake of the Refugee crisis (2015), it has been stipulated that the first state that registers an asylum seeker in this database is responsible for processing his or her application (Aas, 2011, 334). Thus, say, someone who has been registered in Italy and then goes to Norway, and applies another time for asylum, can be sent back to Italy. In this framework, in 2008 the Norwegian police recorded 280 migrants who, in order to avoid the recognition by the EURODAC system and consequently being deported, had disfigured their fingers. 78 of them were imprisoned for the whole duration of their recovery (Nettavisen, 2009). As Aas (2011) notes, "[t]hese experiences show the darker side of the digital body, which is the physical body in pain" (342).

These practices clearly show potential drawbacks and ethical problems of biometrics, since the same practice (taking fingerprints) could be convenient for some but a nightmare for others. But what are the philosophical arguments to back up such criticisms to biometrics and identity? To show this perspective, and in turn critique it in the third chapter, we need to do a step back.

2.2 Conceptual clarifications of identity

In § 1.1, I defined identity "as the state of being the same (or identical) of persons and things". However, it seems that the issue is far more complicated. Not only because there can be different (competing) criteria to define 'being the same', but also because, in everyday language, we use the word 'identity' with different meanings attached to it. Following van der Ploeg (1999), there are at least two distinct senses for which identity is philosophically at stake in biometrics. These two senses are, according to her, *analogous* to the distinction between 'verification' and 'identification' sketched in the previous chapter (§ 1.2).

As a reminder, 'identification' implies the investigation into a wide range of personal data to select a unique individual, while 'verification' just implies the comparison of two data to determine whether they apply to the same person. Technically speaking, while 'identification' involves a one-to-many match, 'verification' involves a one-to-one match.

By analogy, for van der Ploeg, questions of identity in the philosophical literature are concerned with issues of 're-identification' versus issues of 'self-knowledge' (Schechtman,

1990). The former, also known as *quantitative* identity and a typical approach of analytic philosophers, deals with finding out the necessary and sufficient conditions for saying that "a person X at time t1 is the same as X at t2". The latter, or *qualitative* identity and typical of ethicists and social philosophers from the continental tradition, "refers to the beliefs, values and desires that are 'expressive of who one really is'" (Schechtman, 1990, 71). In sum, the first concept is more about what are the criteria that make a person the same throughout time and space, while the second is concerned with *who* one really is, what makes her unique and distinctive (van der Ploeg, 1999, 39).

I believe that the analogy between philosophical (qualitative/quantitative) and technical distinctions (identification/verification) drawn by van der Ploeg (1999) is interesting but only partially correct.

To improve and clarify the analogy, let me make some concrete examples. The first part of the analogy is between issues of identification and self-knowledge. Both inquiries try to reply to the question "who am I" or "who is that person"? In this sense, there is something special or peculiar that makes me who I am and not another person. For instance, being a philosophy student and loving sports belong to my identity, while being a woman and living in London do not (Shoemaker, 2015). It is important to note that, thus conceived, one's personal identity can be contingent: the properties that define one as a person change over time and are flexible. For instance, I can say that now I am different from who I was at 14 years old: I am more sensitive and mature, I have developed different tastes in music and books, I like different sports, and so on.

This flexibility of the concept could contrast with the 'identification' made by identity management systems. From the perspective of the state, or the entity that controls borders, it is not possible to completely leave up to people to write their own autobiographies and make up their identity. Some facts about individuals need to be standardized and out of the control of the individual (Manders-Huits & van den Hoven, 2008, 90). For instance, national identity, ethnic group or sex, which are given to me at birth, can remain relatively fixed throughout time, for example on my ID document or passport (Ludwig, 1997). This happens despite the fact that I could 'feel' myself a man instead of a woman (or the other way round) in case of transgender people or that I could 'feel' myself of another nationality because I grew up in a different country or culture.

The second part of the analogy also needs clarification. Issues of verification in a technical sense are not necessarily analogous to issues of re-identification analysed by analytical

philosophers. Following Olson (2015), this latter group is concerned with at least two questions.

1) Persistence, i.e. what it takes for a person X to persist from time t1 to t2 rather than ceasing to exist. Suppose that you point to an old photo of yourself and say: "This is me". What makes you the same one as the one in the picture? Did the same person persist through time or are we talking about two different entities?
Historically, these questions are related to the idea that we might continue to exist after life (not only in the Christian tradition, but among the Greeks, see Plato (1993)). This is related, for instance, to the question whether biological death (or cerebral death) necessarily bring someone's existence to a conclusion. Today, in the field of bioethics, these questions are particularly relevant in limit cases such as a permanent vegetative state (DeGrazia, 2005). Does a person continue to exist when her cerebral activity is drastically reduced or when she cannot (in any measurable sense) show signs of consciousness?

2) Evidence, i.e. "how do we find out who is who"? What evidence do we need to show whether a person X in this room is the same as the individual Y that was here a month ago? The most common answers found in the literature are two. One is psychological continuity or memory: the person X is the same as Y because she shares with her first-person memory. The other is physical continuity: X is spatio-temporally continuous with Y, that is, X has continued to look like and occupy the same space as Y continuously from t1 to t2.

Olson (2015) makes it clear how (1) and (2), despite the apparent similarity, are two different questions: one is ontological and the other epistemic. "What it takes for you to persist through time is one thing; how we might find out whether you have is another. If the criminal had fingerprints just like yours, the courts may conclude that he is you [Think again of the case of Martin Guerre, and what could have happened if fingerprints were in use at that time]. But even if that is conclusive evidence, having your fingerprints is not *what it is* for a past or future being to be you: it is neither necessary (you could survive without any fingers at all) nor sufficient (someone else could have fingerprints just like yours)."
In sum, to return to van der Ploeg's point, I generally agree about the analogy between technical and philosophical distinctions about identity. However, she fails to acknowledge that re-identification issues are more analogous to *epistemic* questions rather than to *ontological* questions of metaphysical inquiries. I think this is an important point to make:

while current discussions in (bio)ethics of identity are mostly concerned with ontological issues of persistence (end of life ethics or abortion for instance), I believe that epistemic issues of evidence are more relevant to the ethics of biometrics.

2.3 The role of the body as identifier

In the light of such distinction, are both of these concepts of identity (that is, qualitative and quantitative) relevant to biometrics practices? From the perspective of a biometrics supporter, one could argue that philosophical inquiries about personal identity are not at all relevant for identity management. In particular, it could be claimed that I) metaphysical inquiries into the criteria of personal identity throughout time are abstract and not applicable to practical concerns; II) biometrics are more concerned with issues of re-identification rather than identification, and it is not interested in delineating one's alleged 'true' or 'essentialistic' identity. This is supported by the fact that one's biographical and subjective identity (i.e. who I 'feel' I am) is certainly important, but, say, the border guard is not concerned with the issue of *why* X is not allowed in a country, but only *that* X is not allowed.

With the help of the arguments of SSC, I will show how this position is problematic on two fronts.

I) First, let us temporarily assume that qualitative identity issues (i.e. the 'who' questions) actually do not matter for biometrics (I will return to this, however, in II). Nevertheless, biometrics supporters are actually concerned with metaphysical issues of re-identification, since they implicitly assume a physical criterion of personal identity. In fact, this position has seen a growing number of supporters in recent years, and is known as *animalism* (Shoemaker, 2015). In short, the idea is that persons *are* their bodies, or more generally biological organisms or human animals.

Accordingly, the "Biological Criterion" of Personal Identity could be formulated as follows: if X is a person at t1, and Y exists at any other time, then X=Y if and only if Y's biological organism is continuous with X's biological organism (DeGrazia 2005; Olson 1997).

This criterion is in line with our common ways of identifying (and re-identifying) persons (Behrensen, 2014, 48). I usually recognize my friends, say, by their face, voice or gait. The biometrics industry has been trying to 'enhance' these common strategies of identification (e.g. voice and facial recognition) by combining them with other bodily features like fingerprints, iris or DNA.

A criticism that could be made to this approach is that our body goes through drastic changes throughout time and space (van der Ploeg, 2011, 31). In general, body parts can be damaged (e.g. burned fingerprints or face scars) or lost (e.g. a hand), but also new features can be added (e.g. a tattoo). Moreover, many limits have been pointed out regarding how our fingerprints or facial features could change due simply to aging (van der Ploeg, 2012, 181). In the ORIGINS project for instance, one of the biggest obstacles for introducing biometrics identifiers in breeder documents is that it is very difficult to find stable biometric identifiers: fingerprints in new born babies will hardly been consistent in a lapse of 20 years. In general, in some countries (Italy for example) an e-passport has to be renovated every ten years, which is a lapse of time sufficient for drastic changes in one's aspect.

As a counter-reply, a biometrics supporter could bite the bullet about the lack of 100% reliability of a biometric identifier, if used singularly. However, she could remind us the distinction between strong and weak biometrics: some biometrics parameters are more reliable than others (think of DNA) and, when used in combination, they can practically count as certain (§ 1.2).

Therefore, biometrics supporters exclude the psychological criterion or they do not find it important for identity management. Why do they do so? Why is the body so relevant for them? How could the psychological criterion be relevant in biometrics technologies? SSC have put significant effort in trying to answer these questions (Aas, 2006; Ajana, 2010; Amoore, 2006; Lyon, 2003; 2008; van der Ploeg 1999; 2012).

It seems that, for biometrics supporters, the psychological criterion as evidence is not as reliable or 'objective' as the bodily one. For example, in front of a border guard, one could lie and tell a false story (for instance that she is a refugee instead of an economic migrant, or that she is another person than she actually is), but it is harder to fake bodily features (Aas, 2006, 144). As Aas put is (2006):

"Biometric solutions, their proponents suggest, are almost impossible to forge because our bodies, or rather the information extracted from our bodies, are unique tokens of identification. We could call them natural passwords or identity cards that we all carry with us at all times and that we can never forget at home, whether we like it or not. The body, therefore, 'does not lie'" (145).

Aas (2006) and Ajana (2010) agree on how biometric supporters implicitly claim a form of Cartesian dualism but in a reversed way. This time it is not the mind that dominates over the

body, but the other way round: the mind is deceiving while the body is 'truthful' (Aas, 2006, 154).

In one way, there is something valuable to the framework of biometrics supporters, as van der Ploeg herself admits (1999, 42). In the wake of postmodernist accounts of the self, gender studies and virtual realities, it seems that a 'disembodied' idea of 'who we are' is conveyed and that the body is not relevant to our personal identity. Particularly in the literature on virtual identities (e.g. Turkle, 1995) the type of subjectivity purported by Information Technology is de-centred and with uncertain boundaries. For instance, cyberspace and the Internet can allow a person to have multiple identities and play as fictional characters, which are only partially related to one another (think of avatars or virtual selves in gaming). By contrast, scholars from the field of embodied cognition have suggested that other parts of the body besides the mind-brain play a significant causal role in our cognitive and emotional processes (Johnson, 2008). It has been argued how, contra our intuitions, what we refer to as 'mind' is intertwined with and co-shaped by our body, i.e. the two cannot exist apart from each other (Johnson, 2008, 167). In other words, the body is not a simple 'carrier' of our interiority, or hardware where the software of the mind is (contingently) implemented. Our being 'embodied' shapes who we are, how we think and how we feel. Metaphisically speaking, this idea can be related to Aristotle's *hylomorphism* (influential also in Medieval philosophy), which claims that every physical object is a compound of form and matter (Ainsworth, 2016; Ghilardi & Keller, 2012, 39).

However, the focus on the body of biometrics supporters, differently from scholars such as Johnson, risks falling into the extreme opposite, becoming almost a 'fetishism' of the body. According to SSC, such extreme focus on the body is unjustified and morally dangerous. This worry brings us to the second point of the criticism.

2.4 Reductionism and social sorting

II) Second, as van der Ploeg has already shown (1999), the two concepts of identification/verification are more related than it seems, i.e., it is difficult to trace a clear-cut line between the two *and* they are both relevant in the case of biometric identification.

Let us make the case of biometric passports. Quite obviously, passports are important to verify one's identity. When a person X goes to an e-gate, the machine matches the data of X in the database (stored fingerprints and facial image in the case of ABC4EU) with the actual features registered on the spot by the biometric readers. In this sense, X's identity is 'verified': X who is passing through the gate is the same X as the one in the database.

However, even just a simple verification "always implies that an identification procedure has taken place at some time" (van der Ploeg, 1999, 39). 'Verification' of identity can be sufficient to determine whether or not a person is entitled to cross the border (or benefit from a service) *only insofar as* this eligibility has been established before (van der Ploeg, 1999, 40). The biometric data on my e-passport that I use to cross an ABC 'verify' that I am indeed Simone Casiraghi (and not another person who is pretending to be me) but also 'identify' me as an EU citizen who is entitled to cross such a border.

Consequently, although biometrics seem to be not concerned with the 'who' question, they do have an effect on such questions. Biometrics in fact *create*, and possibly 'impose', identities on people (Ajana, 2010, 249). In other words, biometrics not only recognize one's identity, but also have an active role in *constituting* it.

The major criticism by SSC is that there is a risk of reductionism in such practices (Aas, 2006, 153; Ajana, 2012, 242; Amoore, 2006, 344; Lyon, 2008, 507). This is because the aim of biometrics supporters is to 'simplify' the complexity of meaning and function of the concept of identity, to be able to 'read' it more effectively and efficiently. In particular, technological discourses and practices "tend to convert the subjective, and in many ways, profound dimensions of identity into hyper-empirical and objective programmatic Boolean operations of true/false, positive/negative" (Ajana, 2010, 239). The general aim is to 'fix' what is ambiguous, unstable and ever changing that for so long has made practices of identification so unreliable. To put it differently, biometric systems reduce the 'who' question (self-knowledge, qualitative identity) to the 'what' question (re-identification, quantitative identity).

As a result biometrics do not address people as "whole persons with a coherent, situated self and a biography, but rather make decisions on the bases of singular signs" (Aas, 2006, 155). This idea is echoed by Ajana (2010), who notes that "to replace the story with the template, to replace listening with scanning, is akin to *amputating* the possibility of "feeling with" (Marta, 1997, 206) and *castrating* the opportunity of exposing selfhood and uniqueness" (251) (italics added).

Why do these authors use such strong terms like 'amputation' or 'castration' to refer to practices that are apparently innocuous and meant to facilitate our lives? The answer is that SSC have in mind particular categories of 'exposed' and vulnerable people who might experience inequalities with biometrics, like asylum seekers.

Their main political target has been labelled 'social sorting', a concept introduced by Lyon (2003) to which I already hinted with the two examples in § 2.1. The basic idea is that

contemporary biometrics practices have a "classifying drive", similar to past identification practices, but more powerful and disruptive (Lyon, 2003, 13). This, per se, could seem innocent or morally unproblematic, since human life in general needs categorization and tools that allow/deny access to people are necessary for social life (Lyon, 2003, 21). Yet, if we go back to asylum seekers, their case is particularly dramatic and relevant, since these persons are considered 'identity-less', meaning unidentified or unidentifiable, as they do not possess any document of identity. This idea assumes that:

"[B]ehind the notion of identity loss is that identity is something detached from one's self, having an objective and thing-like quality, like money, for example. Describing asylum seekers as 'identityless' therefore presupposes that they do not have the kind of identity required by state bureaucracy: a stable, objective, unambiguous and thing-like identity. The kind that now can be given to citizens, asylum seekers or Afghan refugees by new technological solutions" (Aas, 2006, 147).

What is given them, however, is a 'second-class' identity that stigmatizes them as dangerous or criminals, in other words 'different' from EU citizens (Aas, 2011; Amoore, 2006, 338).

2.5 Theoretical alternative: narrative bioethics

Are biometrics technologies intrinsically problematic then? Is there an alternative to promote a more ethical use of them? As I interpret SSC, it seems that although the use of biometrics is highly controversial (for the whole biometric industry is based on fallacious assumptions on the body and identity), no serious alternative is available at the moment. This quote is particularly explicit:

"Without this shift in the political imaginary, asking the policy-maker to give up biometric control in favour of narrative ethics would be like asking a vampire to give away her fangs to the dentist. Nevertheless, instead of resorting to cynicism, one can, as a starting point, intervene by demonstrating how such policies do not only fail but also worsen the situations they seek to remedy" (Ajana, 2010, 256).

Biometrics are seen as a 'chance' for scholars to reflect on the ways in which biopolitical power and mechanisms of social exclusion are exercised (Aas, 2006; Amoore, 2006), and, in turn, to raise the awareness of "entrepreneurs, researchers and pundits" about the 'who'

question of identity that seems to be forgotten in digitalized practices of identity management (Lyon, 2008, 507). To this end, Ajana talks about a 'bioethical challenge' of biometrics technologies, as

"The challenge to defend ipse-identity, that self-attesting dimension of who someone is, from institutional impositions—especially when those who "inflate" and "launch" enforced forms of identity are chiefly the politicians, policy makers, technical experts, industry representatives […] who, in the name of security and public interest, gather together to decide which identities are worthy of the name and which identities are disposable, implausible, if not even exterminatable" (2010, 249).

In sum, Ajana aims to make room for subjective personal stories in identity management practices, in contrast to standardized 'objective' identities imposed by biometrics systems purported by institutions such as the EU.

Addressing this challenge would in turn help to change the 'general' mentality towards migration and security issues. I believe the most intriguing and elaborated attempt in this sense is Ajana's reference to "narrative bioethics of biometrics" (2010, 249).

This approach is a form of ethics that employs the concept of 'narrative' as both the basis and the object of moral reflections while facing issues of (bio)technologies (Ajana, 2010, 250). The importance of the subjective narration of our experience has already found many supporters in the biomedical field, where the authority of traditional top-down medical ethics has been challenged by the complexity of patients' personal experiences. This bottom up approach could make physicians more responsive towards the sufferance of patients instead of 'imposing' a detached and objective medical treatment (Brody, 1997; Montello, 1997). To give an example, it could be morally justified for a doctor to suspend the therapy of a terminally ill patient given her request not to impose chemotherapy on her.

According to Ajana (2010), the narrative approach could help us to rethink the ethics of biometrics (250), which is nowadays dominated, as I stated in chapter 1, by discourses on privacy. Such discourses, Ajana tells (2010), remain anchored to the traditional "universalistic approaches to ethics" which are "confined to the very same reductionist definitions of identity in which the question of who is all too often diluted into the question of what" (250). As an alternative, the narrative approach could shed more light (as in biomedical ethics) on the personal stories of those whose biometric features are being collected, *in primis* asylum seekers. In these cases, the narrative bioethics, by giving form and sound to the refugees'

voices, would be an ethics of listening and suffering-with, an ethics of sympathy and "responsibility towards the story".

Despite the theoretical interest it raises, it is not immediately clear how such approach would be practically relevant or applicable in the field of identity management. In another work, Ajana (2006) hints at Derrida's politics of generosity based on the ethics of hospitality and proposes a "total exposure to alterity rather than self-ensclosure and fear of otherness" (259). To justify the urgency of her argument she shows how the European policies on migration and biometrics technologies to make them effective are paradoxical; on the one hand, they purpose freedom and democracy, but on the other exclusion and discrimination (260).

In practical terms, although she herself admits the difficulty of thinking her theory under this lens (2006, 271), this sounds to me like a hint to get rid of biometrics practices once and for all. Moreover, it looks as if she is envisioning a utopian border-less society, where immigrants are 'unconditionally hosted':

"[R]egardless of whether they are TB/HIV negative or not, whether they are skilled migrants or not, whether they would contribute to the economy or not, whether they would conform to the customs and values of the host entity or not. This notion of hospitality entails a responsibility that has no limits, no particularity, and an absolute openness to the Other that goes beyond any expectation, determination and knowledge" (Ajana, 2006, 270).

To conclude this chapter, I must admit I sympathize with a narrative account of identity and I find it important that SSC have brought to the table the issue of identity when addressing the ethics of biometrics. However, I believe that, without delving too much into the political implications of these arguments, two main conceptual criticisms could be made. 1) SSC generalize too much from specific cases (e.g. asylum seekers) failing to counter-balance the positive value and/or other ethical problems that could be associated with biometrics in other areas. 2) They fail to provide a serious alternative to current identity management systems (i.e. is it viable to get rid of biometrics and implement a border-less society?). Addressing and developing these points will be the main task of the next chapter.

Notes

[1] The idea derives from the notion of ‘biopower’, which indicates an extension of the power of the state over the physical bodies of its citizens (Foucault, 2009).

[2] For an overview of trusted traveller programs in the US see Higgins (2017).

3. A different take on the ethics of biometrics

3.1 The case of Benjaman Kyle

Before addressing the criticisms to SSC, I want to tell a real story that could be a counter example to their argument, or that at least could trigger the reader's intuitions in another direction (Behrensen, 2017).

In 2004 in Richmond Hill, Georgia, a Burger King employee found an unconscious man behind the restaurant's dumpster. The man was naked, had many physical injuries and his health was restored in the following months by hospitals and shelters. However, even when he gained full consciousness, he could not remember anything before the accident except for some small fragments of his childhood. In general, his most recent memories dated back not later than 1985. Afterwards, he was diagnosed with retrograde amnesia. To make things worse, he had no identity documents on him when he was found, and nobody was able to identify him. In other words, it could be said that the he had lost his identity.

The man, who was assigned the name Benjaman (with an 'a') Kyle, attracted national interest and had to go through many vicissitudes before being able to 'know' who he was. Many attempts by the FBI to reconstruct his genetic genealogy were initially unsuccessful, and authorities refused to issue him a new identity. As a result, lacking a social security number, he could not be employed, access public resources like libraries, rent an apartment or buy a phone card. A documentary shot in 2011 helped him to draw further attention to his case and finally, in 2015, Banjaman announced on his Facebook profile that his genetic relatives and former identity were found (11 years after the accident).

It is true that in part Kyle's identity was lost because his past memories were lost. According to a psychological criterion of identity, he could not be 're-identified' because the psychological link between his 'former self' and his 'current self' was missing (Behrensen, 2014, 46). According to a narrative criterion, he did not have any personal or biographical story to tell about himself that could provide a basis of identification. Does this mean that he was not the same person as, say, when he was a child? Intuitively, I would tend to say no; not only because he still had some weak memories of his childhood, but also for another reason, that is, there could have been some 'external' evidence that could have proven his identity.

If he had a biometric ID or passport with him when he was found, in fact, the story would have been different. A proponent of biometrics might say that, were his biometrics features stored and linked to his name, his identity would have been restored in little time (Behrensen, 2014, 46). Even though Benjaman would not have had any biographical continuity with his

re-stored identity (due to his amnesia), he could have enjoyed the benefits of it (having a job, being able to rent a place, etc.). As Behrensen (2017) notes, in practical and moral terms "what seemed much more devastating *to him* was the lack and the loss of recognition, both personal and official, in the aftermath of his amnesia" (4). It appeared that what mattered for his identity was not just memory or genetic/bodily persistence or evidence (quantitative identity), nor a biographical story (qualitative identity), but that there were other people and institutions "that [could] hold [him] in [his] identity regardless of how [his] physical and mental life might change" (Behrensen, 2017, 4).

3.2 The anthropological view: a third way

Cases like Benjaman Kyle's and Martin Guerre's suggest that, philosophically and practically, identity is not just a matter of intrinsic metaphysical properties (memories, autonomy or rationality, genetics, bodily features, etc.). Rather, what we call 'identity' depends on the extrinsic conventions and social processes we establish as well (even if not entirely on those). In the Guerre case, Martin and the impostor looked alike (there was almost no way to physically establish who was the 'real' one), but Martin 'proved' his identity thanks to the relationships, habits and secrets he shared with relatives and villagers. In the Kyle case, Benjaman's relevant memory *and* documents were lost (and thus could not work as a reliable criterion of identification), and his identity was restored not when he gained memory again, but when his relatives recognized him, thanks to the help of the documentary and social media networking.

If extrinsic elements play such a role in the construction and verification of our personal identities, does this mean that the latter concept is *just* a contingent construction? This is a serious concern, since if personal identity was a mere construction, it would be important for biometrics and identity management only insofar as people generally believed so.

Is there a theory that would be able to account for these characteristics and be useful to add nuances to the ethical debate on biometrics? A 'third way', besides constructionism and metaphysical essentialism of identity, could be pursued. A more fluid theory, which allows for accepting independent evidence while also accepting both intimate and administrative narratives as *normative* frames of personal identity, could add new perspectives to the contemporary debate on biometrics.

To grasp what I mean by 'third way', let me borrow an example from Behrensen, who talks about the philosophy of biology dispute on the ontological status of sex and gender (2017, 33). This debate, she argues, has epistemic and practical relevance, since it concerns the

norms and practices by which we classify people according to their (perceived) gender [1]. On the one hand, there is a realist position that holds that sex consists of purely biological 'facts' (e.g. type of chromosomes or hormones) and these facts 'determine' the gender roles in society. On the other hand there is a constructivist position that argues that gender is a pure social convention and it is independent from biological facts. Both these positions, Behrensen argues, are equally naïve (2017, 33). Even if gender can be conceived as 'social' and sex as 'biological', this does not mean that the two can be easily decoupled and considered independently (Mikkola, 2011). Both positions assume that there exists a dichotomy: either sex and gender must be biologically 'proven' or they must be (artificially) socially constructed. By contrast, one could argue that sex and gender are "a system of social organization bounded by biological elements" (Behrensen, 2017, 34). Sex and gender can be conceived more 'pragmatically' looking at their normative function, which is to impose an order and maintain our social reality.

The theory purported by Schechtman (1990; 2010; 2014) makes analogous considerations for identity: a quantitative criterion (biological or psychological) and issues of *re-identification* of personal identity cannot be separated by a qualitative social reality (issues of *self-knowledge*) associated with the concept (Schechtman, 1990 and § 2.2). Like sex and gender, personal identity offers a normative function to order interpersonal relationships, law or art, and this dimension cannot be ignored.

Schechtman's account could be labelled the 'Anthropological View of personal identity'. Shoemaker (2015) summarizes this view as following: "[o]n the Anthropological View, we are human beings, with ways of life organized around a particular paradigm: We are creatures who typically *develop* and are treated in certain ways not only with respect to our inborn biological and psychological features but also with respect to our *socially shaped capacities*" (italics added).

I believe that it is worth stressing two key concepts of this definition.

1) First, the idea of 'socially shaped capacities'. Among these capacities there are the 'forensic' capacities listed by John Locke, related to responsibility and prudential concern (1975, § II.27.26). Still, these capacities are not to be considered in isolation: we are born into societies "whose members treat us in various ways, giving us names, dressing us, singing to us, taking walks with us, and so on" (Shoemaker, 2015). With this regard, Schechtman (2014) talks about a "socio-cultural infrastructure" as basis for personal identity. This term "is meant to capture the notion of a society as an organization in which humans […] live together

according to established rules involving institutions of support and authority (this can range from tribal or clan organizations to the modern state)" (Schechtman, 2014, 114).

2) Second, the concept of development or 'Person-life trajectory'. The idea is that people go through a standard parallel development of cognitive, agential and 'socially shaped' capacities (from more passive to more active social interactions for instance) as two sides of the same coin. In order to develop certain psychological and physical features you need a certain environment to mature in, and vice versa (Schechtman, 2014, 112). In Shoemaker's words, "[t]hese concerns all track the very same metaphysical unit that gradually *becomes* responsible and concerned for its own future. We thus cannot say that the later responsible unit is a different thing, or even a different kind of thing, from the infant from which he or she developed" (2015).

It must be noted that what Schechtman has primarily in mind with this theory are the bioethical debates about end of life, abortion or advanced directives (2010, 275). Her primary concern is to overcome a dichotomy between "person making capacities" and "animal features", which would lead to separate metaphysical and ethical concerns of personal identity [2]. As a reply, she argues that the loss (or decline) of person-like capacities like rationality or autonomy, for instance in the case of a person affected by dementia, cannot eliminate tout court the web of relationship and interactions one has with others (Schechtman, 2010, 277) [3].

How could this theory of identity be applied to biometrics though? Is it enough to challenge SSC's paradigm? With regards to (1), biometric systems of identity management could be part of Schechtman's idea of "socio-cultural infrastructure", or, to stress the technological component, socio-technical infrastructure. This technological component of biometrics must not be intended as a mere neutral tool for identification (and possibly surveillance purposes) that is able to capture (objectively) a metaphysical essence of people. Instead, biometrics technologies are embedded in a larger set of identity practices that could contribute to develop one's person-life trajectory (2). The biometric data on my passport, for instance, allowed me to travel outside the EU and have certain experiences that defined who I am; and the issuance of this document, that allowed me to do so, was at the same time made possible by a chain of administrative practices.

At first sight, one could remark that Schechtman's theory applied to biometrics is not in open contrast with SSC. Instead, SSC would fully agree that identity is constructed through

biometrics technologies. For this group of scholars, biometrics technologies not only verify identities, but also help constituting them. With this regard, Ajana uses the term 'recombinant identities' (2010) to show the flexibility of the concept that cannot be reduced simply to a 'metaphysical' fact but can be informed by practices and technological development (246). Similarly, Ceyhan (2008, 116) and van der Ploeg (2009, 88) talk about biometrics as a "politics of technological construction of identity", where this process of co-creation is intimately related to the body.

However, what I find problematic is that such construction and constitutive process for an SSC implies a *reduction*, which is always suspicious and morally bad (Ajana, 2010, 252; Lyon, 2008, 507). In this way, their writings give the impression of assuming that (1) there is indeed a 'whole' or 'true' identity of a person that awaits recognition; (2) the individual has a privileged access to it introspectively and eventually decides what her 'true' identity is.

To further criticize these points, I need to delve into the concept of narrativity.

3.3 Criticism to SSC: reductionism

3.3.1 Narrativity

In § 2.5 I talked about narrative ethics, which is based on the concept of narrative, that is, the subjective narration of our experience. This approach often presupposes a narrative criterion of personal identity, which could be defined as follows (Shoemaker, 2015): "What makes an action, experience, or psychological characteristic properly attributable to some person (and thus a proper part of his or her true self) is its correct incorporation into the self-told story of his or her life".

I believe that the concept of narrativity is a promising one to describe personal identity in biometrics practices. However, some accounts of narrative identity, presupposed by some SSC and to some extent by Schechtman (Baylis, 2012, 118), seem to have a too static idea of narrativity. In particular, as Aas portrays it (2006), it risks becoming a 'psychological' and solipsistic criterion. In other words, what she seems to have in mind is some first person and introspective narratives, especially when she talks about asylum seekers and their personal struggles. To quote her:

"Immigration authorities, faced with immigrants and asylum applicants possessing nothing but their stories are, with the help of technology, able to produce an identity 'that is independent of that story, and yet undeniably belonging to that person' (van der Ploeg, 1999,

300). Identity is therefore not established on the basis of self-knowledge and a biographical narrative that an individual can present about him/herself. Rather, it is non-verbal and implemented through symbols that are completely empty of meaning. […] Technological 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, 154-155).

A biometric supporter could argue that this version of biographical narrativity would not work for identification practices, as it is 'subjective' and can be false. One of Strawson's arguments (2004) can be used to support this intuitive idea. In short, he argues how some narratives could just be wrong or completely one-sided: one could see her narrative 'bigger' or different than it actually his, or miss some important details of the story, for instance as a result of traumatic experiences (Strawson, 2004, 447). Additionally, it seems that such account presupposes a Lockean psychological criterion of identity (Locke, 1975, § II.27.15). To put it differently, in order to be able to build such narrative, one would need to have a set of 'higher' cognitive capacities like self-consciousness or rationality (Shoemaker, 2015). This latter point can be especially problematic for some bioethical cases like patients with dementia or very small children.

However, it could be replied to Strawson, also to integrate Schechtman's theory, that narratives do not necessarily have to be introspective: also others have 'stories' about you that could contribute to delineate your identity. Narratives are actually interpersonal, as they include first plus third person perspectives, which mutually co-shape each other (Baylis, 2012, 115). By adding this element, for purposes of identification, one would have to check a person's 'story' against other third person narratives. This happens, intuitively, also in everyday life. For example, if a new friend of mine starts telling me crazy stories about his travels, I could become suspicious and ask other common friends to confirm such stories. Such an approach would be more suited for the bioethical cases mentioned in the paragraph above: while a foetus or a patient with dementia might not possess first person narratives about themselves, others (such as their relatives) would do; one can have a narrative without being able to produce one.

This combination of first and third person narratives works not only in recognition practices between single persons, but also at an institutional level, in identity management practices. Third person narratives in fact, not only include intimate or private narratives (i.e. of other

people) but also administrative and public stories, including those established for example, in the case of Benjaman Kyle.

A concrete example of mixed first-third person narrativity in this sense could be one's CV (Behrensen, 2017, 41). A CV is a narrative form of one's identity that is commonly used for jobs applications: it contains essential information about a person that are useful to characterize her and show that she is suitable for a job. What there is on one's CV is not decided just on the basis of introspection (although this can be an important part of it), but also on social conventions, personal achievements and titles that can be double checked by third parties to be considered trustworthy.

This appeal to third person narratives though brings about another problem, i.e. that of the 'many narratives objection'. If we bring third person narratives to the mix, what happens when there are competing narratives? (Shoemaker, 2015). To give an example, I can be a 'different' person in a variety of contexts: more serious and disciplined at the university, more shy with a group of strangers but more confident with my oldest friends. In a way, I play 'different' roles at school, with friends or with family. One can have even more disconnected private lives, where these roles seem incompatible. Think of a Nazi soldier who is a very caring father but also a guard at a Jewish concentration camp.

Is this argument really a menace to the 'unity' of our 'whole' identity? Is there even such a unity at all? The conceptual clarifications made by Henschke could help to disentangle this puzzle.

3.3.2 Essentialised identity

When he talks about identity in his book, Henschke (2017) introduces two concepts that are useful to the discussion, i.e. that of 'relative equivalence' and 'essentialised identity'.

First, he points out that, when one is making an identity claim about persons, she is making a claim of 'relative equivalence', i.e. "an evaluation that there is *some* equivalence (or sameness, similarity, commonality and so on) between two (or more) things" (Henschke, 2017, 100; italics added). Second, he offers a taxonomy of *at least* 4 different concepts of identity: numeric, character, group and essentialised identity. The first three concepts can be assimilated to the ideas already developed by Schechtman (1990; 2014). Roughly, numeric identity would correspond to issues of re-identification (i.e. what are the conditions under which X at time t1 is the same X at time t2?); character identity would correspond to issues of self-knowledge (i.e. what am I like?); finally, the idea of group identity is in line with the idea of socio-cultural infrastructure of Schechtman (Henschke, 2017, 102-104).

Essentialised identity instead is a difference concept. To grasp its relevance and difference with group identity, I could describe X as an 'environmentalist anarchist vegan'. By saying that, I am acknowledging the social realm and community that makes X the person she is (i.e. her group identity). I am not saying that she has always been an anarchist (she could have also been sympathizing for far right movements, say, in her teenage years), neither that she is 'just' that (she has also other qualities), but I am saying that I identify her with a sort of anarchist type (Henschke, 2017, 105). Conversely, through the concept of 'essentialised' identity, we abstract from a person some specific identifiers or a narrow set of group identity attributes, rather than more generic socio-cultural descriptors (Henschke, 2010, 445). For instance, we could simplify the complex behaviour and traditions of Maoris with reference to the "warrior gene" which was more commonly found in members of that ethnic group (Henschke, 2010, 446). In this case, some could argue that Maoris are more likely to use weapons and exercise violence because of an essentialised genetic trait.

Why are Henschke's reflections relevant for biometrics technologies? From the discussions above it is clear how 'essentialising' a person or referring to her social group could have negative outcomes. Given the historical treatment of minorities, a reductionist account could reinforce discrimination. In the case of migrants and asylum seekers, labelling them as 'dangerous' or 'strangers' from the start could associate them with stereotypes and simplify too much the complexity of their character identity. These persons could become simply these 'facts' about themselves (like the 'warrior gene' for Maoris).

SSC are definitely right in pointing out these risks for people like asylum seekers, but their focus appears too ideologically laden. To clarify, their arguments against biometrics seem driven by their critical ideals concerning current EU migration policies. By focusing mostly on specific cases, they fail to balance their point of view with other contexts of use (other than border crossing), and they do not consider counter-examples to their arguments. For Ajana, the main bioethical challenge for biometrics is:

"[A] matter of heightening policy-makers' awareness that fighting against unwanted immigration and asylum with technology or otherwise only ends up producing an even more unmanageable chain of problems, such as people trafficking, death at the border, and exploitation. And this is perhaps the tragedy of contemporary forms of governance: the more problems they try to solve, the more problems they create" (2010, 256).

The danger of their position is to neglect other areas where biometrics could be beneficial or controversial for different aspects (e.g. what about the management of social services and health records?). I believe that 'essentialising' a person is not per se morally problematic. In fact, Henschke (2017) makes precisely the example of biometrics with this regard (105). If X is 'reduced' to her fingerprint or retinal scan, this is used to give her access to a particular place (e.g. a building) or service. Saying that X is relatively equivalent to Y (say, her fingerprints) is not to say that X is Y and nothing more *in any context*. In saying X is equivalent to Y, "equivalence is *relative* to the given identity concept being used in the context of use", i.e. for instance, when she uses an e-gate to cross a border (Henschke, 2017, 106).

To link Henschke to the Anthropological view of Schechtman, when biometrics practices 'essentialise' one's identity in a certain context, they are not necessarily reducing her identity or threatening the 'unity' of it, but they are using a technology to 'construct' another identity and bring more 'narratives' to the mix in different contexts (in particular, the third-person type). To make my claims less abstract, let us go back to what I already mentioned in § 1.1: that is, that the idea behind identification practices is to make citizens 'legible' for the state with a system of independent checks. Administrators, security forces and border guards need to be able to identify people without having to rely on citizens' local knowledge, but they need a complex apparatus to do so. Robertson (2009) talks about an 'archival' problematisation of identity, as a project where knowledge about individuals is stored in registers (now digital) that can be accessed by agents of the state in order to verify one's identity. This knowledge has to be decontextualized since it has to be understood by someone "who is not familiar with the person in front of them and their unique history and circumstances" (Behrensen, 2017, 86). This type of knowledge is certainly different from the narrative form of 'intimate' and personal knowledge supported by some narrower accounts of narrativity. The state and its institutions also create their narratives: through travel histories, tax payment histories, medical records and so forth. For instance, through its registers a state could build the narrative of X as a reliable citizen since she always paid her taxes on time and did not cheat. As Behrensen puts it (2017), "these histories seem dry and lifeless compared to the narratives we find in intimate contexts […], but they are no less important and their status as narratives is no less meaningful for a moral and practical understanding of personal identity" (86).

Therefore, the problem for migrants and asylum seekers (and other marginalized groups as well) is more nuanced than a reduction of their identity. Indeed their personal stories (moving

to a different country and culture, leaving their family and job) could not be acknowledged, or their bodily features 'taken' forcefully by the state and used to control them, while giving privilege to other groups in society. Yet, despite these potential drawbacks (that SSC have the merit to point out), biometrics could also be beneficial for such marginalized groups, by giving to people that are not 'readable' by the state another identity which would allow them to benefit some services (like having a regularly paid job, insurance, bank account, etc.).

At this point, an SSC might make an objection. She could admit that biometrics do create new narratives for people, but the problem is that such narratives become the only ones used by those in power. Biometrics supporters might not believe that the person is merely their fingerprints/stereotypical descriptor, but they are treating that person *as if* she is no more than her fingerprints/stereotypical descriptor.

I agree about this point (this is exactly why Henschke is partially worried about essentialised identity), and I believe that here my positions and that of SSC could get closer to each other. But biometrics must not be confused with something that menaces per se the 'unity' of someone's identity; indeed, the point just raised is more about power rather than identity strictly speaking. What it is needed, ethically, is to make sure that the possible damages resulting from this 'essentialisation' made by biometric identity management systems are kept to a minimum. To highlight this point, I will focus on epistemological issues coming from biometrics technologies in the next section.

3.4 Epistemological and moral issues

To look into the epistemology and morality of biometrics under a different lens from SSC, let me go back to the distinction between epistemological/ethical issues of what it is meant by 'objectivity' (§ 1.3). As a recap, biometrics technologies can be intended as more objective technologies in two ways: morally, they produce more 'impartial' outcomes; epistemologically, they produce more sound forms of identification. I will show, through Behrensen (2017), how these two aspects are actually interrelated: on the one hand, having a certain moral 'expectation' of impartiality is based on a certain epistemic stance; on the other, having a 'foundationalist' epistemic 'project' of identification can account for some moral issues of identity management.

3.4.1 Epistemological loopholes in the identity chain

To recap, from an epistemological point of view, SSC's critique mostly focus on the role of the body: for biometrics supporters, the information 'extracted' from it would have a (non-

justified) privileged epistemic status for identification purposes (Ajana, 2010, 244; Aas, 2006, 145; Ceyhan, 2008, 116; Lyon, 2008, 504; van der Ploeg, 1999, 42). But this is not the main moral fault of the arguments portrayed by biometrics supporters. The alleged 'soundness' typical of biometrics identification also derives from a precise project of knowledge building that goes from more 'basic' to more complex facts. In my opinion, this project is seen too much ideally, and its practical limitations are not taken into account enough, as I demonstrate below. In sum, SSC fail to acknowledge epistemological loopholes in identity management practices, which I consider the weakest spot in the arguments of biometrics supporters.

Following Behrensen (2017, 87), it could be argued that there are two epistemic overarching goals of identity management systems: i) they aim to be closed systems (i.e. completely self-referential) [4] and ii) they wish to 'essentialise' personal identities to basic facts (e.g. list of names, dates of birth, fingerprints stored in IDs, etc.).

As for (ii), to go back to the ORIGINS project mentioned in § 1.4, one of the most 'basic' facts about people's identity are the data in breeder documents like birth certificates. Such documents in fact are the basic 'bricks' that allow people to apply for IDs, passports, driver licences and to vote, for example. However, as already pointed out, there can be gaps in this 'identity chain' that goes from birth to (eventually) death certificates. For instance, miscommunications, failed transfer of information from one office to another or lack of readable information could present obstacles to identification practices. To make a personal case, while I was working at the airport of Lisbon at ABC4EU, it took me a while to exit the 'flights connection' area where I was doing surveys with travellers because I did not have a passport with me but only an Italian ID card. Since this document is still paper based (even if perfectly valid as a travel document within EU), the border guard was at first very suspicious, while my colleagues used their digital Spanish ID and quickly exited the area through e-gates. Situations like these suggest that these systems are open (i.e. their boundaries are porous and flexible), and not closed (i).

To support this point, Behrensen (2017) makes a parallel with the two traditional (opposing) schools of epistemology: foundationalism and coherentism. These approaches try to answer the question 'how are our beliefs justified?' (or 'how can one say that X *knows* a proposition p?') using different strategies. In short, coherentists argue that a belief is justified (or unjustified) insofar as it is coherent (or incoherent) with my system of beliefs. For example, my belief 'X is a funny person' is justified because coherent with my other beliefs like 'X is cheerful', 'X makes good jokes', 'X is smart', and so on (Pritchard, 2006, 37). By contrast, foundationalists argue that a belief is justified not on the basis of its content, but on the basis

of the structure of my belief system. In practice, we hold some basic beliefs (which do not need justification because self evident) as well as some derivative beliefs, which can be justified by inference from basic beliefs. This strategy can be traced back to Aristotle and Descartes, but also, more recently, to Russell or the Vienna Circle. To give an example, my belief "it is a good idea to play basketball today" can be based on more basic beliefs like a) the weather forecast says it is going to be 25 degrees; b) the sky from my bedroom window looks clear; c) the weather forecast and the clear sky suggest that the weather is perfect to play some ball (Pritchard, 2006, 39).

To make a parallel with identity management systems, how do we know whether one's identity claims are justified? In this framework, it appears clearer how the 'ideal' of modern-states identity practices (that is, the one endorsed by biometrics supporters) is foundationalist (Behrensen, 2017, 89). In other words, any identity verification should be justified on more basic facts, that is biological samples, IDs, passports or breeder documents. Birth certificates, in particular, and the administrative acts of creating legal persons, are the root of the whole chain. The 'identity chain' functions like this: I can apply for an ID if I have a breeder document, for a passport if I have an ID, etc. Ideally, this identity chain should be 'perfect' to work. However, in practice, this is not the case. For example, breeder documents are easy to falsify, which would lead to the possibility to apply for a secure e-passport, say, with a counterfeit birth certificate. Moreover, birth certificates across the EU do not conform to international standards yet (Behrensen, 2017, 93).

Practically speaking, identity management systems do not function in a foundationalist way. In fact, they have to 'correct' their defects by interfacing with other systems of knowledge, with a process of feedback loop. To integrate Behrensen's reflection on the topic, I believe that these systems can be explained following a holistic strategy of coherentism, as presented by Quine (2013). In general, holism refers to the fact that it is not possible to understand a thing without looking at the larger whole where it is situated. Without going into details, the so-called Duhem-Quine thesis argues that it is not possible to test a hypothesis (or scientific theory) in isolation; instead it is only possible to test such theory *plus* a whole network of assumptions and claims that come with it (Gillies, 2013, 271; Quine, 2013, 264). To grasp this idea, let me make an historical example taken by Gillies (2013). In 1845 two astronomers discovered that the orbit of the planet Uranus around the Sun was not in accordance with the one predicted by calculations, derived from Newton's law of gravitation. Instead of rejecting the whole theory, the astronomers modified the assumptions behind the theory, postulating

the existence of another planet (which was later discovered as Neptune) that would explain the observed deviance in Uranus' orbit (Gillies, 2013, 272).

To continue the analogy between epistemology and identity management, biometric identification systems use, in fact, holistic types of justification instead of foundationalist ones. To prove our identities, they cannot rely only on biological samples 'in isolation' collected by biometrics identifiers such as ABCs. These biological samples, instead, only make sense as a part of an intricate network of knowledge kept together by identity management systems. In such systems there is no strict hierarchy: biological samples are not 'truer' than other sources of information about people such as names, addresses or gender.

An example of this 'holism' of identity management systems could be refugee status determinations (RSD). In these cases, lawyers and administrators have to establish whether, on an individual basis, the asylum seeker's claims are credible and justified. The UN Refugee Agency (UNHCR) has developed some procedural guidelines to go through the process (UNHCR, 2003). This process cannot be done simply and primarily on the ground of more 'basic' facts, such as reading 'bio-data' (5.8) or asking the country of origin alone. Rather, it involves balancing carefully many other elements, such as their documents, the claims in their interviews (possibly with the help of an interpreter) or relevant medical information, which are all part of the so-called RSD file (2.6). In turn, interviewers and officers have to go through a careful process of selection and training (4.2) and, for instance, respect the applicant's right to confidentiality (2.1) and be sensitive to age and gender issues (1.3).

Under the lens of Quine's holism RSD is a process based on a 'web' of claims and identifiers. One's application is evaluated on the basis of multiple narratives besides empirical 'biological' biometrical facts, ordered more like a polycentric net than a (hierarchical) ladder. As a result, biometrics are not a technology to blame in itself for its possible discriminatory outcomes, but the identification systems (and its possible flaws) as a whole socio-technical system could be problematic.

It seems that, while too much attention has been given by SSC to reduction of identity and surveillance, epistemic gaps in identity management procedures are also crucial to reflect on moral inequalities coming from biometrics identity systems. It is the presence of these gaps, for instance, that brings about problems of *access* that limit the feasibility of this process. For example, many countries could not afford up to date biometrics technologies. Similarly, persons might not have the resources to buy a biometric passport: in the UK for instance the fee for a passport increased from £5 in 1975 (roughly £40 today, considering inflation) to £75,50 or £85 today, depending on whether you purchase online [5].

This is also, I believe, the main problem for the Aadhaar Indian system mentioned in § 1.4. In a recent article on BBC news, Biswas (2018) argues how this biometric system would actually be "hurting the poor". Many people (especially children), for instance, are deprived of the subsidised food from the state's public distribution system (and consequently die of starvation) not because there are no supplies, but because their ration cards have not been linked to their Aadhaar number. To make things worse, Indian states constantly conduct investigations to cancel allegedly 'fake' ration cards (like Jharkhand in March 2018 that cancelled 760 000 ration cards). Most of them, it is believed, are annulled because not linked to Aadhaar. Similarly, in 2017, when the government made it mandatory to link Aadhaar to pensions, 300 000 'fake' pensions were annulled. Again, it is said, according to some empirical research, that just a fraction of this number are actual 'fakes', thus resulting in genuine pensioners being excluded (Biswas, 2018).

These cases look like a shocking and still on-going ethical problem of biometrics that is not really related to the 'exploitation' of the body and surveillance practices (which is still *an* issue nonetheless), but more to bad administrative practices and epistemic gaps. Still, the fact that so far *Aadhaar* is not meeting the expectations is not due to an intrinsic moral problem of biometrics. Administrative fallacies with the technologies could be improved in the future to achieve some purposes they were originally designed for, like easier tax planning and increased transparency of government actions.

3.4.2 Value-ladeness and biases in identification

Besides these 'administrative' problems, there is another set of moral concerns that has not been widely discussed in the literature on biometrics yet. These types of concern have been widely discussed in the field of philosophy of science and apply well to the discourse of biometrics as a technological solution for identification. To make an example, what if the border guard has prejudices on some asylum applicants, for instance the ones coming from Islamic countries? Would an automated process make identification more objective in the sense of neutral or impartial? To answer these types of question we need to look at the vaule-ladeness of observations and measurements, making a parallel between the (recent) history of philosophy of science and biometrics epistemology (Ghilardi & Keller, 2012).

A biometrics supporter could admit that, in fact, the identity chain systems are incomplete but that, nonetheless, these technologies could help to produce fairer outcomes. Imagine a person X going through a border crossing point at an airport somewhere in Europe, where there had been a terrorist attack a few days before. The perpetrators of the attack are still on the loose. X

has a dark skin and a long black beard, and wears a traditional *thawb*. At the moment of the passport check, the border guard find the person suspicious and takes him apart for further controls. At the end of the check, his identity is double-checked and he is let through. However, for this extra check, X missed an important job interview. By contrast, imagine that X can go through an e-gate. He puts his EU passport and fingerprints on the reader, has his facial image checked and, in less than a minute, he is through and can attend his job interview.

Now, would this latter scenario be more desirable? And why? It seems that an automated process not only could speed up the border crossing, but it could avoid the suspicions (groundless in the case just mentioned) and biases of the border guard based only on prejudices and physical appearance. However, this view of the situation is too simplistic. In fact, the idea of a lack of bias and impartiality of automation has been criticised on many fronts (Friedman & Nissembaum, 1996; Krasmann & Kühne, 2014; Macnish, 2012). To clarify, it must be pointed out that, whenever we talk about automated systems in identification practices, we can refer to two distinct processes: partial automation (the machine filters the information and the human operator decides) and full automation (the machine both filters and 'takes' decisions) (Macnish, 2012, 158).

First, let us assume, for now, that fully automated identification techniques would be feasible in the near future [6]. It appears true that there are several benefits in automating such techniques of identification. For instance, the limited processing capacity of the human operator can make her commit errors or filter out information based on stereotypes. Think of border guards in peak hours at airports: they have to process huge amounts of information and take decisions in a few seconds. The risk of information overload and, consequently, mistakes is very high.

Still, the matter of more fairness of machines (compared to human operators) is not as straightforward as it seems (Macnish, 2012, 158). After all, machines and algorithms are designed by humans, and as such they can embody biases of their programmers. It has already been discussed for instance how, in forensics, DNA databases (which would look like a very 'objective' form of identification) could be discriminatory (Chow-White & Duster, 2011).

In addition, there is the issue of false positives and false negatives (Macnish, 2012, 160). To understand this distinction, imagine the situation of a person P going through an alarm system S placed at the exit of the shop. S detects those that leave the shop without paying for the item X. If P sets off S even if she paid for X, she would be a false positive. By contrast, if P does not set off S but she did not pay for X, and manages to get out of the shop without being

caught, she is a false negative (Macnish, 2012, 155). It is clear that by calling biometrics 'more objective' because supported by automated systems, advocates do not mean that this technology can *completely* avoid false positives and false negatives. Rather, they would argue that, in comparison to human operators, they would lower the number of errors. Yet, the problem is that, with automated systems, the number of false positive and negatives could *increase* due to the limited amount and type of information that the machine can process (Macnish, 2012, 160).

Besides the issues just listed, however, there is a more fundamental problem with full automation. The concept of full automation is a simplification; in reality there is always a mixture between full automation/human operator, or a *continuum* that goes from manual to full automation (Macnish, 2012, 158), and it is still difficult to *imagine* a context where full automation could take place.

In practice, in migration control systems, there is still the need of a person supervising the biometrics machines. Therefore, real-life situations are actually cases of partial automation, which bring about problems of (i) interpretation, (ii) additional epistemic burden.

i) Under this lens, it must be stressed how the human decisions made on the basis of alleged 'objective' data are still the results of processes of attribution of meaning and interpretations (Krasmann & Kühne, 2014, 9). As Ghilardi & Keller (2012) put it, "[i]t would be a naïve error to consider the identity of the object we're dealing with as something unrelated to the way we're going 'to read' it" (41). As Kuhn already showed (1962), every scientific 'fact' is intertwined with observations of it, which in turn are shaped by methods or theories to do them. Similarly, 'facts' about identities that are automatically generated and based on a binary code are not 'objective' because they cannot be separated from the operator's interpretation. In other words, "Just as a colour is not describable from its numerical frequency, but needs to be interpreted to grasp its specific qualitative difference, identity needs to be interpreted and grasped from its quantitative reduction as well" (Ghilardi & Keller, 2012, (43).

ii) Along with the issue of interpretation, it is also not clear that automation would help with dealing with a huge quantity of information and always speed up the process. While I was working for ABC4EU for instance, it often happened that fingerprint readers had problems or were not working at all (e.g. if, for environmental conditions, the travellers' hands were too cold). In those cases, the border guard or police officer had to intervene 'manually' and bypass the process. Digitally processed data, paradoxically, would even *add* an 'epistemical

burden' to process for the border guard instead of diminishing it (Behrensen, 2017, 95). For instance, new border guards have to be able to distinguish between glitches in the systems (like fingerprints errors), problems adjusting the camera for facial recognition or a person trying to deceive the system (for instance with a silicon mask or silicon gloves with fake fingerprints).

In sum, on the basis of the epistemological investigations in 3.4, systems of identity management are 1) open (or not closed) and 2) biased, but this is not a reason to get rid of them (as some SSC would argue) or to add even more technologies (technofix solutions). Instead, recognizing these limits should push us to pay more attention to how these systems are implemented by those with social and *political* power and used by those who do not have that (e.g. asylum seekers) (Behrensen, 2017, 108).

Notes

[1] The issue is also very relevant to the debate about biometrics, gender and border security at airports (see Currah & Mulqueen, 2011).

[2] For Schechtman (2010), theories of personal identity have failed, so far, to provide a metaphysical theory of persons that could make sense of our practical concerns, leading their supporters to have two different theories for practical and metaphysical identity (271). The mistake comes from a too narrow focus on person-like capacities (moral agency, consciousness) and a failure to see how these capacities "are integrated into a larger life" (272).

[3] I do not have the space here to defend in detail such theory of identity or apply it to contexts other than biometrics. The anthropological view is still a 'young' theory, and has been mainly applied to other branches of bioethics. The discussion sketched in this chapter will hopefully give some hints for further elaborations.

[4] To make it clearer, in a closed system every input and output would be known within a specific time, deterministically, and its boundaries are rigid (Stichweh, 2011).

[5] For the prices of passports see: https://www.gov.uk/renew-adult-passport. To calculate historical UK inflation rates: http://inflation.iamkate.com.

[6] I make this assumption because what I want to show is that it is not necessarily the case that moving across the spectrum towards full automation necessarily raises impartiality.

Conclusion

To conclude, I need to make two last steps. First, I would like to recap the main accomplishments of my argument and highlight its strong points. Second, I want to acknowledge two limitations/weaknesses of my position and recommend, as a solution, some future lines of research.

To begin with, this thesis started from the question: "to what extent the study of biometrics technologies through the philosophy of personal identity could offer new perspectives to the existing ethical debate?" I showed how a philosophical analysis of identity could help to look critically to the arguments pro and con biometrics out there. In sum, I argued how in contrast to the optimistic narrative in support of biometrics, the current debate is polarized in a certain direction. To offer nuance to the debate, I tried to bridge the gap between more 'optimistic' technocrats supporters of biometrics and more 'pessimistic' accounts of SSC. What I suggested is that biometrics identification is not per se morally problematic, but at the same time its limitations should be responsibly acknowledged. This is especially evident in the case of India, where an entire welfare state system based on biometrics has been introduced. On the one hand, biometrics supporters should be more aware that the choices they make and the policies they enforce are loaded with political and philosophical assumptions that could be morally problematic. On the other hand, critics of biometrics should not simply focus on the negative sides of biometrics (e.g. bodily surveillance) and on their reductionist outcomes.

To demonstrate my point, I dedicated the first chapter to a terminological and historical analysis. Delving into definitions and types of biometrics has helped to grasp the main characteristics and possible advantages of these technologies. A brief historical overview of identity management practices and identity documents allowed me to introduce the rationale behind the current use of biometrics in the EU and India. In the second chapter, I turned to the mainstream criticism of biometrics purported by SSC. Despite the different backgrounds of these authors, I argued how they tend to see biometrics as an example of 'gloomy' surveillance technology that takes the body as an infallible (*quantitative*) criterion of personal identity. Since SSC assume that there are also *qualitative* characteristics pertaining our identities (i.e. our biographical stories), biometrics are not able to capture the 'whole' identity of people but make them appear as 'less' than *who* they really are. In turn, this reduction could lead to discrimination and social sorting, especially in the case of more vulnerable categories like asylum seekers. In the third chapter, I criticized SSC arguments for 1) their idea of identity, too much based on an introspective and qualitative concept of narrativity; 2) their excessively ideologically driven account, which leads them to focus just on a particular

group (asylum seekers) and ignore other (possibly positive) applications. As for (2), by broadening the analysis to the institutional embeddedness of identity management, I showed how the discriminatory practices could be the result of 'epistemological loopholes' in the 'identity chain' that are not sufficiently acknowledged. As a concrete case, instead of talking about migration and asylum seekers, I addressed the current expectations and difficulties around *Aadhaar*, like the case of 'fake' pensions.

As for (1), I drew on Schechtman 'anthropological' account of identity (2014) to show how the idea of 'reduction' of biometrics identification is misplaced: biometrics actually add more interpersonal narratives to the mix instead of flattening one's 'whole' identity. The *recognition* (or its absence) by others, individuals as well as institutions, plays a key role in constituting one's identity; in fact, it is worth mentioning that there are many points in common between Schechtman and political theories of recognition (e.g. Taylor, 1992). For both, identity is 'negotiated' intersubjectively, and non-recognition can inflict harm and oppression. Still, I find Schechtman account more valuable as she combines logical-metaphysical and ethical-political concerns of identity, whereas recognition theorists tend to ignore the metaphysical debate (Iser, 2013; McQueen, 2018). However, insights from recognition theory could be valuable for future research to assess the impact of biometrics on other vulnerable groups, such as queer or transgender people (Currah & Mulqueen, 2011).

Finally, I want to point out two limitations of my work. First, my analysis looked mostly into how institutions influence biometrics and the concept of identity in an almost instrumental way; but it is worth noting that the process also goes the other way round (Vermaas et al., 2011). Institutional settings are in turn shaped by new technologies, and I recommend that scholars focus on this angle to add insights to the current debate.

Second, I have mainly discussed the interrelation of epistemological, metaphysical and ethical issues of biometrics and identity. It results from my discussion, however, that also political factors are involved. By focusing on positive sides of biometrics, at this point, one could be tempted to go even a step further. My whole discourse seems to presuppose the necessity of the role of the state for identity management procedures. But what if this role is put into doubt? What if identity management could be possible without a centralised state? These technologies could not only be a means to control citizens, but also one to empower or liberate them from the state itself. In particular, Mordini & Massari (2008) suggest how "biometrics technologies also promise to liberate citizens from the 'tyranny' of nation states and create a new global, decentralized, rhyzomatic schemes for personal recognition" (496).

It is very important to note that this argument pro biometrics must not be confused with the arguments sketched in chapter 1. The latter are arguments from a more 'technocratic' perspective, which focus on aspects of security, speed and convenience. The argument elaborated by Mordini & Massari is instead from a broader political perspective, and seems to suggest that these technologies could help us overcome 'traditional' nation-based identification practices. While today the states hold the power to create national identities, thanks to the construction of bureaucracies and infrastructures for that purpose, this situation could be changed.

The use of brand new information technologies, which are more and more de-centralized, coupled with an increasing number of identity-less people crossing EU borders, but also with situations in the Global South, where traditional identification schemes are absent or poorly implemented [1], could open up new scenarios. Private actors and independent agencies instead of huge governmental structures, in fact, could take control of biometric systems (as it is already happening in some parts of the world, such as in the African and Asian market). In fact, these processes per se do not need centralised structures but could be implemented by a network of local or private institutions (Mordini & Massari, 2008, 497). Consequently, a new figure of the 'global citizen' could emerge and be based on a solid identity management system independent of nation states.

This is certainly a suggestive and controversial view, but I think that, at the present state of technological development it is too early to draw such conclusion. To investigate this idea, I recommend that future research look into biometrics markets and applications in the context of developing countries, where a solid infrastructure of national identity management systems is lacking. For now, delving into expectations and future perspectives of biometrics (in particular, second-generation ones) goes beyond the scope of this thesis, but could certainly be a promising follow-up interdisciplinary research.

Notes

[1] In 2000 UNICEF calculated that 50 million babies around the world were not registered at birth and thus lacked identity documents. Pakistan, Bangladesh and Nepal for instance, have not made child registration at birth compulsory yet (Mordini & Massari, 2008, 497).

Bibliography

- Aas,K. F. (2011). 'Crimmigrant' Bodies and Bona Fide Travellers: Surveillance, Citizenship and Global Governance. *Theoretical Criminology, 15*(3), 331-346.
- Aas, K. F., Gundhus, H. O., Lomell, H. M. (eds.) (2009). *Technologies of InSecurity. The Surveillance of Everyday Life*. London and New York: Routledge.
- Aas, K. F. (2006). 'The Body Does Not Lie': Identity, Risk and Trust in Technoculture. *Crime Media Culture, 2*(2), 143-158.
- Achterhuis, H. (ed.) (2001). *American Philosophy of Technology. The Empirical Turn* (R. P. Crease Trans.). Bloomington and Indianapolis: Indiana University Press.
- Ainsworth, T. (2016). Form vs. Matter. The Stanford Encyclopedia of Philosophy (Spring 2016 Edition), E. N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2016/entries/form-matter/>.
- Ajana, B. (2010). Recombinant Identities: Biometrics and Narrative Bioethics. *Bioethical Inquiry, 7,* 237-258.
- Ajana, B. (2006). Immigration Interrupted. *Journal for Cultural Research, 10*(3), 259-273.
- Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography, 25,* 336-351.
- Baylis, F. (2012). The self in situ: A relational account of personal identity. In J. Downie & J.J. Llewelyn (eds.), *Being Relational: Reflections on Relational Theory and Health Law* (109-131). Vancouver, BC: UBC Press.
- Behrensen, M. (2017). *The State and the Self. Identity and Identities.* London: Rowman & Littlefield.
- Behrensen, M. (2014). Identity as a convention: biometric passports and the promise of security. *Journal of Information, Communication and Ethics in Society, 12*(1), 44-59.
- Bigo, D. (2014). The (in)securitization practices of three universes of EU border control: Military/Navy – border guards/police – database analysts. *Security Dialogue, 45*(3), 209-225.
- Biswas, S. (2018, March 27). Aadhaar: Is India's Biometric ID Scheme Hurting the Poor? *BBC News.* Retrieved from: https://www.bbc.com/news/world-asia-india-43207964
- Brody, H. (1997). Who gets to tell the story? Narrative in postmodern bioethics. In H. L. Nelson (ed.), *Stories and their limits: Narrative approaches to bioethics* (18-30). New York: Routledge.
- Bromba, M. (2007). Biometrics Animals. Retrieved from: http://www.bromba.com/knowhow/BiometricAnimals.htm

- Castells, M. (1999). *The Information Age: Economy, Society and Culture.* Oxford: Wiley-Blackwell.
- Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society, 5*(2), 102-123.
- Chow-White, P. A., Duster, T. (2011). Do Health and Forensic Databases Increase Racial Disparities? *PLOS Medicine, 8*(10), 1-3.
- Cole, S. A. (2001). *Suspect Identities. A History of Fingerprinting and Criminal Identification.* Cambridge, Massachusetts: Harvard University Press.
- Currah, P., Mulqueen, T. (2011). Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport. *Social Research, 78*(2), 557-582.
- Dahl, J. Y. (2009). Another Side of the Story: Defence Lawyers Views' on DNA Evidence. In K. F. Aas, H. O. Gundhus, H. M. Lomell (eds.), *Technologies of InSecurity. The Surveillance of Everyday Life* (219-237). London and New York: Routledge.
- Daugman, J. (2014). 600 million citizens of India are now enrolled with biometric ID. *SPIE Newsroom,* 1-4.
- De Grazia, D. (2005). *Human Identity and Bioethics.* Cambridge: Cambridge University Press.
- Friedman, D., Nissembaum, H. (1996). Bias in Computer Systems. *ACM Transactions on Information Systems, 14*(3), 330-347.
- Foucault, M. (2009). The History of Sexuality. London: Penguin Books.
- FRONTEX (2014). *Annual Risk Analysis 2014.* Warsaw: Poland.
- Garfinkel, S. (2000). *Database Nation. The Death of Privacy in the 21st Century.* Sebastopol, California: O'Reilly Media.
- Gasper, D. (2009). Global Ethics and Human Security. In H. Fagan, R. Munck (eds.), *Globalisation and Security: an Encyclopaedia.* Westport, CT: Praeger.
- Ghilardi, G., Keller, F. (2012). Epistemological Foundation of Biometrics. In Mordini, E., Tzovaras, D. (eds.), *Second Generation Biometrics: the Ethical, Legal and Social Context* (23-48). New York: Springer.
- Gillies, D. (2013). The Duhem Thesis and the Quine Thesis. In M. Curd, J. A. Cover, C. Pincock (eds.), *Philosophy of Science. The Central Issues* (271-287). (Original work published 1993).
- Heimo, O. I., Hakkala, A., Kimppa, K. K. (2012). How to abuse biometric passport systems. *Journal of Information, Communication and Ethics in Society, 10*(2), 68-81.

- Henschke, A. (2017). *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.
- Henschke, A. (2010). Did You Just Say What I Think You Said? Talking about Genes, Identity and Information. *Identity in the Information Society, 3*(3), 435-456.
- Higgins, M. (February 20, 2017). Which 'Trusted Traveler' Program Is Right for You? *The New York Times.* Retrieved from: https://www.nytimes.com/2017/02/20/business/which-trusted-traveler-program-is-right-for-you.html
- ICAO (2015). Machine Readable Travel Documents. ICAO/Document 9303, retrieved from: https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf
- Iser, M. (2013). Recognition. In E. N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2013 Edition), URL = <https://plato.stanford.edu/archives/fall2013/entries/recognition/>.
- Jain, A. K., Kumar, A. (2012). Biometric Recognition: an Overview. In Mordini, E., Tzovaras, D. (eds.), *Second Generation Biometrics: the Ethical, Legal and Social Context* (49-79). New York: Springer.
- Johnson, M. (2008). What Makes a Body? *Journal of Speculative Philosophy, 22*(3), 159-169.
- Koon, W. K. (November 18, 2016). The complex origins of Chinese names demystified. *South China Morning Post.* Retrieved from: https://www.scmp.com/magazines/post-magazine/long-reads/article/2046955/complex-origins-chinese-names-demystified
- Krasmann, S., Küne, S. (2014). My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society, 12*(1), 1-14.
- Kuhn, T. (1962). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.
- Locke, J. (1975). *An Essay Concerning Human Understanding* (P. Nidditch, ed.). Oxford: Clarendon Press. (Original work published 1694).
- Ludwig, A. M. (1997). *How Do We Know Who We Are?* Oxford: Oxford University Press.
- Lyon, D. (2009). Identification Practices: State Formation, Crime Control, Colonialism and War. In K. F. Aas, H. O. Gundhus, H. M. Lomell (eds.), *Technologies of InSecurity. The Surveillance of Everyday Life* (42-58). London and New York: Routledge.
- Lyon, D. (2008). Biometrics, Identification and Surveillance. *Bioethics, 22*(9), 499-508.

- Lyon, D. (2003). Surveillance as Social Sorting: Computer Codes and Mobile Bodies. In D. Lyon (ed.), *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination* (13-30). London and New York: Routledge.
- Macnish, K. (2012). The Unblinking Eye: the Ethics of Automating Surveillance. *Ethics and Information Technology, 14,* 151-167.
- Malafouris, L. (2008). Beads for a Plastic Mind: the 'Blind Man's Stick' (BMS) Hypothesis and the Active Nature of Material Culture. *Cambridge Archaeological Journal, 18*(3), 401-414.
- Manders-Huits, N. (2010). Practical Versus Moral Identities in Identity Management. *Ethics and Information Technology, 12,* 43-55.
- Manders-Huits, N., van den Hoven, J. (2008). Moral Identification in Identity Management Systems. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato (eds.), *The Future of Identity in the Information Society* (77-91). Boston: Springer.
- Marta, J. (1997). Towards a bioethics for the twenty-first century: A Ricoeurian poststructuralist narrative hermeneutic approach to informed consent. In H. L. Nelson (ed.), *Stories and their limits: Narrative approaches to bioethics* (198-214). New York: Routledge.
- McQueen, P. (2018). Social and Political Recognition. *The Internet Encyclopaedia of Philosophy*. Retrieved from: https://www.iep.utm.edu/recog_sp/
- Meijers, A. (ed.) (2009). *Philosophy of Technology and Engineering Sciences.* Amsterdam: Elsevier.
- Mikkola, M. (2011). Ontological Commitments, Sex and Gender. In C. Witt (ed.), *Feminist Metaphysics* (67-83). Dordrecht: Springer.
- Montello, M. (1997). Narrative competence. In H. L. Nelson (ed.), *Stories and their limits: Narrative approaches to bioethics* (185-197). New York: Routledge.
- Mordini, E. (2014). Biometrics. In H. A. M. J. ten Have, B. Gordijn (eds.), *Handbook of Global Ethics* (505-526).
- Mordini, E., Tzovaras, D. (eds.) (2012). *Second Generation Biometrics: the Ethical, Legal and Social Context*. New York: Springer.
- Mordini, E., Massari, S. (2008). Body, Biometrics and Identity. *Bioethics, 22*(9), 488-498.
- Mordini, E., Petrini, C. (2007). Ethical and Social Implications of Biometrics Identification Technology. *Annali dell'Istituto Superiore di Sanità, 43*(1), 5-11.
- Murphy, E., Maguire, M. (2015). Speed, Time and Security: Anthropological Perspectives on Automated Border Control. *Etnofoor, 27*(2), 157-177.

- Nettavisen (2009) *Flere fjerner fingeravtrykkene*. Retrieved from: http://www.nettavisen.no/innenriks/ article2584898.ece
- Olson, E. T. (2015). Personal Identity. In E. N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Summer 2017 Edition), URL = <https://plato.stanford.edu/archives/sum2017/entries/identity-personal/>.
- Olson, E. T. (1997). *The Human Animal: Personal Identity Without Psychology*. New York: Oxford University Press.
- Pappas, T. S. (2016). The Specter Haunting Europe. Distinguishing Liberal's Democracy Challenges. *Journal of Democracy, 27*(4), 22-36.
- Pécoud, A., Guchteneire, P., de (2006). International Migration, Border Controls and Human Rights: Assessing the Relevance of a Right to Mobility. *Journal of Borderlands Studies, 21*(1), 69-86.
- Plato (1993). *Phaedo.* (C. J. Rowe ed.). Cambridge: Cambridge University Press.
- Ploeg, I., van der, (2012). The Body as Data in the Age of Information. In K. Ball, K. Haggerty and D. Lyon (eds.), *Routledge Handbook of Surveillance Studies* (176-183). London and New York: Routledge.
- Ploeg, I., van der (2011). Normative Assumptions in Biometrics: On Bodily Differences, In-built Norms, and Automated Classifications. In S. Van der Hof and M. Groothuis (eds.), *Innovating Government—Normative, Policy and Technological Dimensions of Modern Government* (29-40). The Hague: TMC Asser Press.
- Ploeg, I., van der (2009). Machine-Readable bodies: Biometrics, informatization and surveillance. In E. Mordini et al. (eds.), *Identity, security and democracy* (85–94). Amsterdam: IOS Press.
- Ploeg, I., van der (2007). Genetics, Biometrics and the Informatization of the Body. *Annali dell'Istituto Superiore di Sanità, 43*(1), 44-50.
- Ploeg, I., van der (1999). Written on the Body: Biometrics and Identity. *Computers and Society,* 37-44.
- Pritchard, D. (2006). *What is this thing called knowledge?* London and New York: Routledge.
- Quine, W. V. O. (2013). Two Dogmas of Empiricism. In M. Curd, J. A. Cover, C. Pincock (eds.), *Philosophy of Science. The Central Issues* (250-270). New York: W. W. Norton & Company. (Original work published 1951).
- Redpath, J. (2007). Biometrics and International Migration. *Annali dell'Istituto Superiore di Sanità, 43*(1), 27-35.

- Robertson, C. (2009). A Documentary Regime of Verification: The Emergence of the US Passport and the Archival Problematization of Identity. *Cultural Studies, 23*(3), 329-354.
- Schechtman, M. (2014). *Staying Alive. Personal Identity, Practical Concerns, and the Unity of Life.* Oxford: Oxford University Press.
- Schechtman, M. (2010). Personhood and the Practical. *Theoretical Medicine and Bioethics, 31,* 271-283.
- Schechtman, M. (1990). Personhood and Personal Identity. *The Journal of Philosophy, 87*(2), 71-92.
- Shoemaker (2015). Personal Identity and Ethics. *The Stanford Encyclopedia of Philosophy* (Winter 2016 Edition), E. N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/win2016/entries/identity-ethics/>.
- Stichweh, R. (2011). Systems theory. *International Encyclopedia of Political Science.* New York: Sage.
- Strawson, G. (2004). Against Narrativity. *Ratio, 17,* 428-452.
- Taylor, C. (1992). The Politics of Recognition. In A. Gutmann (ed.), *Multiculturalism: Examining the Politics of Recognition* (25-73). Princeton: Princeton University Press.
- Torpey, J. (2001). The Great War and the Birth of the Modern Passport System. In J. Caplan and J. Torpey (eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World* (256-270). Princeton: Princeton University Press.
- Torpey, J. (2000). *The Invention of the Passport. Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press.
- Thomas, R. (2005). Biometrics, Migrants and Human Rights. *The Online Journal of the Migration Policy Institute.* Retrieved from: https://www.migrationpolicy.org/article/biometrics-migrants-and-human-rights
- Turkle, S. (1995). *Life on the Screen. Identity in the Age of the Internet.* New York: Simon and Shuster.
- UNHCR, (2003). Procedural Standards for Refugee Status Determination under UNHCR's Mandate. Retrieved from: http://www.unhcr.org/4317223c9.pdf
- Vermaas, P., Kroes, P., van de Poel, I., Franssen, M., Houkes, W. (2011). *A Philosophy of Technology. From Technical Artefacts to Sociotechnical Systems.* San Rafael, CA: Morgan & Claypool.

- Wayman, J. L. (2007). The Scientific Development of Biometrics Over the Last 40 Years. In K. de Leuw and J. Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook* (263-274). Amsterdam: Elsevier.
- Woodward, J., D., Jr., Webb, K. W., Newton, E. M., Bradley, M., Rubenson, D. (2001). *Army Biometric Applications. Identifying and Addressing Sociocultural Concerns.* Santa Monica, CA: Rand.