

HELLE STENUM

THE BODY-BORDER – GOVERNING IRREGULAR MIGRATION THROUGH BIOMETRIC TECHNOLOGY

TECHNOLOGICAL CROSS-OVER

Biometric technology is booming and is being developed in close cooperation between the IT and security industries, academics, engineers and social scientists, and governments around the world investing large sums of public funds to be part of the global biometric system of border control and surveillance. The market analysis company “6Wresearch” announced in 2016 that the global biometrics market was “one of the key growing electronic security markets in the global landscape” and was projected to reach \$ 21,9 billion by 2020. Increasing government spending, national ID projects, e-passports and visas, rising crime rates, growing terrorist activities, cyber crime, and data theft are seen as reasons for spurring the market for various biometric technologies globally.¹

Biometric identifiers (finger prints, facial and iris scans etc.) have increasingly become a key element in technology of EU border and migration management. Proposed by the EU Commission in 2011 and aimed at separating the ‘bona-fide’ traveller in the mobility flow from the ‘risk’ traveller, and facilitating identification and deportation of ir-

¹ Tech in Asia: According to 6Wresearch, Global Biometrics Market is projected to reach \$ 21,9 billion by 2020. Cp. 6Wresearch, “Global Biometrics Market is Projected to Touch \$21.9 Billion by 2020”, *LinkedIn*, Mai 31, 2016. Available at: <https://www.linkedin.com/pulse/global-biometrics-market-projected-touch-219-billion-2020-> [accessed June 27, 2017]. Another market research company projects Biometric System Market worth \$ 32,73 Billion by 2022: “The biometric system market size is expected to increase from USD 10.74 Billion in 2015 to USD 32.73 Billion by 2022, at a CAGR of 16.79% between 2016 and 2022”. Markets and Markets, “Biometric System Market worth 32.73 Billion USD by 2022”, *Press Releases*, n.d. Available at: <http://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp> [accessed November 30, 2016].

regular migrants, “Smart Borders” based on biometric technology have become central in EU management of migration. This development takes place against a backdrop of a booming biometric industry preoccupied with technical solutions on government technology such as national ID, passports and “mobility-access-devices”.

Biometric technology is radically invading commercial² as well as governmental forms of surveillance and the governing of people as consumers and as citizens or anti-citizens.³ A remarkable technological overlap between private marketing and governmental securitization is currently taking place. In the private market for example, the use of a fingerprint to unlock your iPhone is being pushed by Apple, and Facebook has developed a face recognition mechanism alongside their huge database of facial images.

However, public investment in private corporation-based biometrics in migration control has been a significant element in both paving the way for normalising biometric surveillance and establishing the databases and technology that are now praised as securitized access control in all kinds of societal areas.

This paper discusses both recent technological developments in EU migration management, as well as the historical context of biometric technology to explore the apparent biometric divide between citizens and migrants, the latter positioned and managed as risks, through surveillance and data collection, while citizens are managed as hold of access to privileges. The technique of both circuits, however, involves bodily coded information, emphasises the general tendency of “securitization of identity”⁴.

SEEING LIKE A (N IRREGULAR) MIGRANT

A starting point for analysing the effects of biometric technology in migration management is the perspective of the irregular migrant. Documented ‘identity’ is and has always been important for crossing borders,

² Cp. Kartikay Mehrota, “Retailers Experiment With Surveillance Tools Used by Police”, *Bloomberg Businessweek*, March 3, 2016. Available at: <https://www.bloomberg.com/news/articles/2016-03-03/retail-stores-experiment-with-surveillance-tools-used-by-police> [accessed November 29, 2016].

³ Anti-citizen is someone portrayed as a risk to the wellbeing, virtue, norms and values of society – for example criminals and undocumented migrants. Cp. Jonathan Xavier Inda, *Targeting immigrants: Government, technology, and ethics*, Oxford, Wiley-Blackwell, 2005; Sharam Koshravi, *The ‘Illegal’ traveller: an auto-ethnography of borders*, Basingstoke, Palgrave Macmillan, 2010.

⁴ Nikolas Rose, “Government and control”, *British Journal of Criminology*, 40, 2000, pp. 321–339; Nikolas Rose, *Powers of freedom. Reframing political thought*, Cambridge, Cambridge University Press, 1999.

and migrants cross borders with various types of forged documents or without documents every day. However, for the majority of illegalized migrants in the EU, ‘border crossing’ at the external borders took place as a legalized act with their own passports, visa, temporary residence permits etc. and afterwards they overstayed for various reasons or they acted in non-compliance with the residency permits.⁵

Documented ‘identity’ and identification become crucial in the everyday life of illegalized migrants (non-status residents) in order to cope with the condition of *deportability*⁶ and to avoid deportation. To construct, buy or borrow a suitable identity, for a health insurance card for example, can protect you against deportation if you are caught in a police check. However, a “passing identity” can also give you access to gated and privileged communities or member clubs⁷ for legalized residents only – for example in workplaces, hospitals, education etc. One can say that these irregular migrants practice a strategy of ‘flexible identities’.

Flexible Identities and De-identification

Utilising flexible identities during migration is one of many strategies developed to counter or circumvent barriers and state-produced obstacles. Such strategies reflect the current rules and restrictions of the management of migration. Flexible identities can also work as an emigration-strategy to overcome restrictions of transnational management of migration, such as time-limited residence permits, entry bans, or not qualifying for immigration. Buying or borrowing the identity of a resident in the country of origin, for example of a family member or neighbour, can facilitate migration. Obviously this can have unintended consequences for both the migrant travelling as well as for the resident staying in the country of origin. For example, the resident could lose their social rights temporarily because they are documented as having left the country.

Another strategy is “de-identification”⁸, which conceptualises the

⁵ Cp. Martin Ruhs, and Bridget Anderson, “Semi-compliance in the migrant labour market”, *COMPAS Working Paper*, 30, 2006.

⁶ Cp. Nicholas de Genova, “Migrant ‘Illegality’ and deportability in everyday life”, *Annual Review of Anthropology*, 31, 2002, pp. 419–447; Nicholas de Genova, *Working the boundaries: Race, space, and “Illegality” in Mexican Chicago*, Durham, Duke University Press Books, 2005.

⁷ Cp. Dennis Broeders, “Return to sender? Administrative detention of irregular migrants in Germany and the Netherlands?”, *Punishment & Society*, 12 (2), 2010, pp. 169–186, here: p. 47; John Torpey, *The invention of the passport surveillance, citizenship and the state*, Cambridge, Cambridge University Press, 2000, p. 33.

⁸ Kim Rygiel, “Bordering solidarities: Migrant activism and the politics of movement and camps at Calais”, *Citizenship Studies*, 15 (1), 2011, pp. 1–19.

strategy used by irregular migrants in a “return position”. If for example an illegalized migrant is caught by the police with no papers and is not willing to cooperate on his/her return to a country of origin, it can be difficult or impossible to deport the person. According to international regulations based upon the “national order of things”⁹, deportation of a foreign citizen requires that the deportee is identified and recognized by the country of origin. Without papers to identify citizenship, the migrant achieves a condition of de-facto “non-deportability”¹⁰.

The precondition for the flexible identity strategy is that you can attain the (forged or original) proper papers. The precondition for the de-identification strategy is that you get rid of proper documents. In both cases, the migrant operates and strategizes in a space between a bodily and self-identified existence and a governmental representation/identification of a migrant or resident.

To speak in database terminology, she as herself can in principle be linked to more than one state identity, for example, working in different workplaces under different identities or going to hospital under a different identity. From the perspective of the migrant, this can be said to be a *one-to-many relation* between the individual and the representation of the individual by the state, whereas from the perspective of the state, each identity is supposed to match only one individual, bodily existence.

For the resident using the de-identification strategy, the state is not able to produce an identity linked to citizenship and therefore it can be defined as a *one-to-none relation* between resident and nation states.

One-to-many and one-to-none relations both represent counter-conduct towards the dominant governmentality of migration management and more broadly, disorder in the context of nation state government of populations and identity. However, the idea of one-to-one relations between an individual and an identifiable state-based identity, is fundamental in constructing and developing biometric management of migration.

PURPOSE AND FUNCTION CREEPS

To understand the current developments in EU migration management we will look into the proposal to alter the Eurodac Regulation.¹¹ Bio-

⁹ Liisa H. Malkki, “Refugees and exile: From ‘refugee studies’ to the national order of things”, *Annual Review of Anthropology*, 24, 1995, pp. 495–523.

¹⁰ Broeders 2010.

¹¹ Cp. European Commission, “on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for ex-

metric identifiers have increasingly become a key element of EU border and migration management,¹² especially in technology aimed at governing irregular migration and facilitating return and deportation of illegalized migrants. Biometric identifiers have primarily involved fingerprints and facial recognition, but also DNA.¹³

In the EU Prüm system,¹⁴ which builds on an agreement to step up cooperation in the “fight against terrorism, cross-border crime and irregular migration”, fingerprints and DNA are exchanged between member states of charged and convicted persons. SIS II, Eurodac and VIS¹⁵ are centralized systems that contain fingerprints of different groups of non-EU citizens: SIS II stores fingerprints of third country nationals with entry bans for three years; Eurodac has since 2000 stored fingerprints of asylum seekers for 10 years and fingerprints of migrants apprehended at border crossing for two years; VIS contains fingerprints

aming an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (recast)”, *Proposal for a Regulation of the European Parliament and of the Council*, COM(2016), 272 final, May 4, 2016. Available at: <https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-272-EN-F1-1.PDF> [accessed June 20, 2017]; “Eurodac is a computerised system consisting of a central unit, which operates the central database of biometric data, and of a communication infrastructure for transmitting the data between the Member States and the central unit. [...] Member States are required to record the fingerprint data of all persons who are seeking asylum or who have been apprehended crossing the external border irregularly.” EPRS, “Recast EUrodac regulation”, October 2016, not accessible anymore.

¹² Cp. Didier Bigo, Sergio Carrera, Ben Hayes, Nicholas Hernanz, and Julien Jeandesboz, “Justice and home affairs databases and a smart borders system at EU external borders. An evaluation of current and forthcoming proposals”, *CEPS paper in Liberty and Security*, 52, 2012.

¹³ The term Biometrics covers a range of different physical and behavioural elements linked to the body: e.g. fingerprints, face recognition, iris scan, DNA, vein analysis, gait, and heart rhythm.

¹⁴ Based on the Prüm Convention: Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. Cp. Auswärtiges Amt, “Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, Prüm/Eifel, 27 May 2005”, *Auswärtiges Amt*, 2015. Available at: <http://www.auswaertiges-amt.de/cae/servlet/contentblob/607270/publicationFile/165214/Statusliste-EN.pdf> [accessed June 27, 2017].

¹⁵ The Schengen Information System (SIS) is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The Visa Information System (VIS) allows [Schengen States](#) to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. Cp. European Commission, “Schengen Area”, *Migration and Home Affairs*, 2017. Available at: http://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en [accessed June 20, 2017].

of all visa holders for five years.¹⁶

These systems aim to govern both a large group of third country nationals and EU citizens considered to be criminals by the state or anti-citizens. The biometric identifier is stored in order to link a specific body to specific information related to status (asylum seeker, entry banned, convicted etc.). In the digitization or “Information” strategy of the EU Commission on “Stronger and Smarter Borders”,¹⁷ biometric technology is celebrated and characterised by a number of qualities, one of which is: “Biometric technology can reduce the risk of mistaken identities, and of discrimination and of racial profiling”¹⁸.

Recast Eurodac Regulation

The so-called refugee crisis¹⁹ in 2015-16 in Europe has intensified the development of biometric technology aimed at managing populations and the mobility of migrants. In the spring of 2016, the EU Commission proposed to change the criteria for capturing data in Eurodac as one of the measures to regain control of migration to the EU.²⁰ Changing the use of data for a different goal than it was collected for can be characterized as purpose creep.²¹

But the so-called migration and refugee crisis was not the only argument. Two further issues are behind the purpose creep.

The first one aims to govern undocumented migrants in general on EU territory:

“During the same period, those Member States that are not situated at the external borders began to see an increasing need to be able to store and compare information on irregular migrants that were found illegally staying on their territo-

¹⁶ Cp. European Commission, “Overview of information management in the area of freedom, security and justice”, *Communication from the Commission to the European Parliament and the Council*, COM(2010) 385 final, July 20, 2010. Available at: <http://ec.europa.eu/transparency/regdoc/rep/1/2010/EN/1-2010-385-EN-F1-1.Pdf> [accessed June 20, 2017].

¹⁷ Cp. European Commission, “Stronger and Smarter Information Systems for Borders and Security”, *Communication from the Commission to the European Parliament and the Council*, COM(2016) 205 final, June 4, 2016. Available at: <http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-205-EN-F1-1.PDF> [accessed June 20, 2017].

¹⁸ Cp. European Commission, COM(2016) 205 final, p. 4.

¹⁹ Cp. Peter Nyers, *Rethinking refugees. Beyond states of emergency*, London/New York, Routledge, 2006.

²⁰ Cp. European Commission, COM(2016), 272 final.

²¹ Terms often used to describe development of databases containing personal information, here Wisman (2013): “The use of technology to perform a function it was not originally intended for constitutes function creep. [...] The use of data for a different goal than it was collected for results in purpose creep.” Tijmen Wisman, “Purpose and function creep by design: Transforming the face of surveillance through the internet of things”, *European Journal of Law and Technology*, 4 (2), 2013.

ry, particularly where they did not seek asylum. As a consequence, thousands of migrants remain invisible in Europe”²².

The presence of undocumented or irregular migrants is not a new phenomenon and not necessarily linked to the so-called refugee crisis. But the seeing-like-a-state approach²³ tends to encourage efforts to seek an increasing legibility from the perspective of the state – reducing ‘invisibility’ of the subjects and making them governable. Biometric identifiers are a key to legibility.

The second creep aims to facilitate the return or deportation of undocumented migrants in general:

“Facilitating the identification of illegally staying third-country nationals or stateless persons through the use of biometrics would contribute to improving the effectiveness of the EU return policy, notably in relation to irregular migrants who use deceptive means to avoid their identification and to frustrate re-documentation.”²⁴

In maintaining the “national order of things”²⁵, illegalized migrants must be removed from the national territory. Legibility through biometrics will facilitate deportation and order, which emphasise “the gradual hardening of the control tools”²⁶.

The original purpose of the Eurodac in 2000 was to facilitate the Dublin regulation in order to check fingerprints if an asylum seeker has applied for asylum in another EU Member State and the first purpose creep in 2013 gave law enforcement authorities access to EURODAC for anti-terror and anti-serious-crime purpose.²⁷ Another major creep in the purpose and scope of the Eurodac regulation is now on the horizon with the proposed extension of registration to not only include registered data of asylum seekers and persons illegally crossing borders, but now also to facilitate “identifying illegally staying third-country nationals and those who have entered the European Union irregularly at the external borders, with a view to using this information to assist a Member State to re-document a third-country national for return purposes”²⁸. The purpose has crept into a more general technology of governing

²² European Commission, COM(2016) 272 final, p. 2.

²³ Cp. James C. Scott, *Seeing like a state: How certain schemes to improve the human condition have failed*, New Haven, Yale University Press, 1998; Helle Stenum, “Making migrants governable: counting and defining the ‘illegal migrant’”, *Nordic Journal of Migration Research*, 2 (4), 2012, pp. 280–288.

²⁴ European Commission, COM(2016) 272 final, p. 3.

²⁵ Cp. Malkki 1995.

²⁶ Sergio Carrera, and Nicholas Hernanz, “Re-framing mobility and identity controls: The next generation of the EU migration management”, *Journal of Borderlands Studies*, 30 (1), 2015, pp. 69–84, here: p. 71.

²⁷ Cp. European Commission, COM(2016) 272 final.

²⁸ European Commission, COM(2016) 272 final, p. 3.

anti-citizens defined as asylum seekers, potential criminals and terrorists, and non-citizens defined as illegalized non-EU migrants.²⁹

But not only has the purpose crept, functions are also creeping. The proposal suggests a new type of biometric data (facial image) captured from an extended group (irregular migrants and children). Furthermore, the retention period for storing data of irregular migrants has been proposed to be extended from 18 months to five years, and opening up the transfer of Eurodac data to third country authorities is also proposed, in order to:

“use EURODAC data for identifying and re-documenting an illegally staying third-country national for return and re-admission purposes will necessarily entail sharing that data in some circumstances, with a third country”.³⁰

It is proposed that facial images are to be collected and stored in the database together with fingerprints. Reasons for the extension and for using this particular biometric identifier are formulated in terms of efficiency and facilitation of transnational communication between EU member states – and also with non-EU nation states. The argument for lowering the age of biometric identification from 14 to six years is that it could help families in the case of separation.³¹ Finally, it is emphasised that member states are obliged to take fingerprints and capture facial images, and that detention can be used as sanction in case of refusal by the migrants.³²

The use of facial images as stored identifier of a person is different from a fingerprint in various ways; from the ‘gaze of the governor’ it is easier to obtain a facial image (what the industry refers to as “less intrusive”), it facilitates a unique key to surveillance in public and other places, it supports state of the art global biometric identification efforts by governments, such as biometric passports, visa-systems, national ID cards etc., to maintain “the national order of things”³³ where every human being is identified as belonging to a nation state. A facial biometric identifier is much more difficult to spoof or alter than fingerprints and furthermore, as the EDPS (European Data Protection Supervisor) has noted “the unique identifier might be used for other purposes, for example for identifying the individuals in other databases, making the

²⁹ Cp. Inda 2005; William Walters, “Reflections on migration and governmentality”, *Movements. Journal für Kritische Migrations- und Grenzregimeforschung*, 1 (1), 2015, pp. 1–25; Rose, *Powers of freedom. Reframing political thought*.

³⁰ European Commission, COM(2016) 272 final, p. 14.

³¹ European Parliament, “Briefing EU Legislation in Progress”, October 2016, not accessible anymore.

³² Cp. European Commission, COM(2016) 272 final.

³³ Malkki 1995.

comparison of databases easy and simple”³⁴.

BIOMETRIC CITIZENSHIP AND FLEXIBLE ZONES AND GATES

The proposal to creep purpose and function in the Eurodac however, is part of a larger EU agenda on migration management in general, and reforming the Common European Asylum System more specifically.³⁵ Hence, also a proposed Entry/Exit system is designed with a similar logic – especially when it comes to the specific biometric facial identifier.³⁶

The EU Commission proposed in October 2011, the development of new biometric systems that will facilitate management of especially irregular migration through monitoring when an ‘entry’ of a traveller does not match an ‘exit’, alert the authorities about overstayers, help to identify and apprehended an irregular migrant and facilitate deportation.³⁷

In 2013 the proposal was revised and pilot studies, public hearings etc. have been carried out. In April 2016, the EU Commission put forward a new proposal on smart borders. Compared to the 2013 version, the new proposal includes more biometrics, including facial recognition, and extending the retention period from 181 days to five years. Furthermore, the proposal emphasises the importance of “interoperability”, implying the integration of the smart border system Entry/Exit with other anti-citizen systems of the EU. Last but not least, the proposal enables law enforcement to use the border control system and the

³⁴ European Data Protection Supervisor, “EDPS: Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)”, *Opinion 07/2016*, September 21, 2016. Available at: https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf [accessed June 20, 2017], p. 18.

³⁵ Cp. European Commission, “Towards a Reform of the Common European Asylum System and Enhancing Legal Avenues to Europe”, *Communication from the Commission to the European Parliament and the Council*, COM(2016) 197 final, April 6, 2016. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160406/towards_a_reform_of_the_common_european_asylum_system_and_enhancing_legal_avenues_to_europe_-_20160406_en.pdf [accessed June 20, 2017].

³⁶ “The collection of facial images will be the pre-cursor to introducing facial recognition software in the future and will bring EURODAC in line with the other systems such as the Entry/Exit System. Eu-LISA should first conduct a study on facial recognition software that evaluates its accuracy and reliability prior to this software being added to the Central System”. European Commission, COM(2016) 272 final, p. 4f.

³⁷ Cp. European Commission, “Smart borders – options and the way ahead”, *Communication from the Commission to the European Parliament and the Council*, COM(2011) 680 final, October 25, 2011. Available at: <http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-680-EN-F1-1.Pdf> [accessed June 20, 2017].

individual profiling data in the system.³⁸

In addition, a “Registered Traveler’s Program” has also been proposed by the EU Commission, that privileged and “bona-fide travelers” are exempt from waiting in lines at the borders with other more ‘risky’ third country nationals, but subject to the same large scale biometric identifier. This system will result in the EU thereby “extending its capacity to control mobility far beyond its jurisdiction, gathering up personal data from ever more countries in the world”³⁹. In accordance with the tendency to use biometrics in border management, fingerprints and facial images are also integrated in passports in the EU, but the use of this biometric information is for now restricted to simply establishing the link between the body and the passport. Fingerprints are not stored in a central database and linked to other kinds of information.

The vision of the EU Commission can be regarded as an attempt to produce *non-flexible identifiers* in the relationship between mobile individuals and the member states in order to create flexibility at the border and in the territory in order to create *flexible zones and gates*.⁴⁰

The one-to-one state-produced identifier provides the security-focused state with the possibility of using the same identifier to access/deny access to different spaces/zones, and the state can furthermore dynamically change decisions on access simultaneously with changes in status – for both migrants and citizens.

From the perspective of the EU commission the capacity of enforcing a unique one-to-one relation between the body and status will add new elements to the existing technology of governing mobility and migration. It will improve the border-zone control – the pre-departure control, the control on arrival at the border and after arrival in the EU. It improves the possibility of immediate and reliable body-identity checks – in the country of origin, at the border, in the streets of the EU, in the detention centre, at the workplace etc. Scanning of the biometric identifier can take place anywhere – within, between and outside nation states of the EU. Within the EU territory, technological gatekeepers can

³⁸ Cost-benefit is also calculated by the Commission regarding the entry/exit and Frequent Travellers system, predicting that member states “could have a net cost savings already after the second year of operation” stemming from reduction in border control resources by around 40% (equivalent to EUR 500 million/year). Development cost for the first three years and with some of the biometrics added later is estimated to around EUR 390 million, and yearly operational costs in a period of 5 years of operation is estimated to be 189 million EUR. In this 8 year span costs are estimated to be EUR 1,335 million). Cp. European Commission, COM(2011) 680 final.

³⁹ Marie Martin, “Extension of mobility partnerships with euro-mediterranean partners”, *Panorama*, 2012, pp. 279–283, here: p. 281.

⁴⁰ Cp. Walters 2015; Didier Bigo, “Freedom and speed in enlarged borderzones”, in: Vicki Squire (ed.), *The contested politics of mobility: Borderzones and irregularity*, Abingdon, Routledge, 2011, pp. 31–50.

appear in public and private spaces randomly, arbitrarily, planned or fixed to determine the status of individuals and patrol the borders of a zone that may be physical (a building, a workplace, a hospital, a school, a shelter, an ATM) or abstract (access to social benefits, unemployment benefits, application for residence permit, voting etc.).

Biometric identifiers are constructed as non-flexible in order to create the preconditions for flexible borders, zones, channels and gates that can facilitate both the celebrated global, fast-tracked, smooth mobility of humans⁴¹ and the reproduction of the geo-political division of individuals into national populations and the social sorting of residents within and between nation states.⁴² This is a new disturbing infrastructure, which has been characterised as irreversible.⁴³

BIOMETRIC ALIENAGE⁴⁴

In a nation state context, biometric identifiers have primarily been reserved for criminal residents and unwanted foreigners, with the fingerprinting of rejected asylum seekers, deported aliens and illegalized migrants. During the last decade, the EU has however, as we have seen, implemented technological mechanisms to ‘combat’ the possibility of *de-identification* and *flexible identities* through the use of forged documents at the border.

Fraud, false documents, low penalties and corruption are often cited when linking irregular migration to criminal activities.⁴⁵ Within a control regime based on unique identification, a centralised state authority for issuing the required identifications, and a high degree of state access to unique, identifiable data, creates conditions for borders being patrolled, regardless of if these borders are placed at the perimeter of the nation state or if the patrolling and control takes place through individual profiling and random inspections at bus stations or public parks.

The suggestion and implementation of biometric identifiers reflects a move away from the principle of rights applied to human beings as an abstract of the universal idea that all individuals are equal, to a trouble-

⁴¹ Cp. Zygmunt Bauman, *Globalization*, New York, Columbia University Press, 1998.

⁴² Cp. David Lyon (ed.), *Surveillance as social sorting: Privacy, risk, and automated discrimination*, London, Routledge, 2005.

⁴³ Cp. Bigo et al. 2012.

⁴⁴ “Alienage” as defined by Bosniak: “the position of the marginalized non-citizen or the degree of ‘alienage’ are produced by nation-states exercising sovereignty and ‘managing migration’, and framing conditions for mobility and residence of migrants. ‘Alienage entails the introjection of borders’”. Linda Bosniak, *The citizen and the alien*, Princeton, Princeton University Press, 2008, p. 5.

⁴⁵ See for example Frontex, “Smarter, Faster, Safer?”, *Feature Stories*, 2011. Available at: <http://frontex.europa.eu/feature-stories/smarter-faster-safer--KfKGq2> [accessed June 21, 2017].

some concept of rights being engraved in the body, and the body is not neutral, but socially constructed and contextualised in the place of birth, kinship, geography, etc. The use of biometric identifiers in migration management seems to be increasingly important to separate citizens from anti-citizens and non-citizens.

Even though biometric 'body'-borders can be characterized as a new kind of surveillance, Maguire and Amoore emphasise that biometric data in the process of governing mobility is hardly a new phenomenon.⁴⁶ Amoore points to "the historical emergence of body counts to enumerate and account for colonial subjects"⁴⁷. She refers to Appadurai's discussion of systems of classification in colonial India,⁴⁸ where the enumeration and accounting disciplines the "unruly body", bringing it back into a zone of calculation and manageability, recuperating it and accounting for it within 'normal' ranges of acceptability.

"Contemporary biometric body counts bare out much of what Appadurai signals for the creation of 'boundaries around homogeneous bodies' that 'performatively limits their extent', flattening differences and idiosyncrasies into calculable categories. New forms of biometric technology extend this categorisation and enumeration of the body via processes of risk profiling, such that they have themselves come to perform and represent a border that approves or denies access"⁴⁹.

Biometric technology is the materialization of a political thought mutated from practices of government linked to the panoptical perspective of government and to colonial forms of governing through bodily control and identities. One of the current biometric identifiers is fingerprinting, which has been a social technology to measure and identify the criminal body, developed in colonial India and technologized in the era of IT into databases of criminals and suspects.⁵⁰ Another biometric identifier – facial recognition - also has historical links to Bertillon's anthropometry and standardization of mug shots as well as anthropological use of Bertillonage to identify the criminal body in late 1800s.⁵¹ Today biometric passports or databases contain extended and new possibilities of governing through the body and not through representations

⁴⁶ Cp. Mark Maguire, "The birth of biometric security", *Anthropology Today*, 25, 2009, pp. 9–14; Louise Amoore, "Biometric borders: Governing mobilities in the war on terror", *Political Geography*, 25, 2006, pp. 336–351.

⁴⁷ Amoore 2006, p. 342.

⁴⁸ Cp. Arjun Appadurai, *Modernity at large*, Minneapolis/London, University of Minnesota Press, 1996.

⁴⁹ Amoore 2006, p. 342.

⁵⁰ Cp. Simon A. Cole, *Suspect identities: A history of fingerprinting and criminal identification*, Cambridge, Harvard University Press, 2002.

⁵¹ Cp. Cole 2002.

such as ID cards, personal registration numbers, names, etc.

Large scale databases, such as SIS II and Eurodac, containing data of the expelled, the penalized, the overstaying etc. – offers the possibility to select and separate legals from illegals, the deserving from the non-deserving, citizens from unwanted migrants. The “biometric passport” or identifier merges several mutated key technologies of the colonial nation-states such as fingerprints, mug shots and passports into a technical, depoliticised instrument targeting ‘the Others’.⁵² However, with biometric passports, national ID cards, access codes to mobile phones, credit cards using the same standards and technology, the ‘Selves’ are now also included as objects for biometric surveillance and scanning.

FICTIONS OF FREEDOM AND NON-DISCRIMINATION

The primary underlying argument for biometric smart borders is the need for “securitization of identity”⁵³ which is constructed as enhancing “freedom of movement” through “speeding up travel flows” as analysed by Bigo: “[...] under liberal government mobility is translated into a discourse of freedom of circulation, which reframes freedom as moving without being stopped and confuses the speed of well-channeled movement with freedom”⁵⁴.

Biometric identifiers are furthermore falsely constructed as neutral, objective, unforgeable, unique, true identifications of human beings. Several scholars have criticized the fabric of biometric identification for transforming socially-constructed categorizations as technological, neutral data.⁵⁵ Analysing the science that constructs biometrics and failures in biometric identifications, Magnet shows how the technologies rely on culturally-coded constructs of the gendered, racialized, classed and disabled body.

“Biometrics are marketed as able to eliminate systemic forms of discrimination at the same time they are produced in a

⁵² Cp. Cole 2002; John Torpey, *The invention of the passport surveillance, citizenship and the state*, Cambridge, Cambridge, Cambridge University Press, 2000.

⁵³ Rose 1999; 2000.

⁵⁴ Bigo 2011, p. 33.

⁵⁵ Cp. Shoshana Amielle Magnet, *When biometrics fail: Gender, race, and the technology of identity*, Durham/London, Duke University Press, 2011; Joseph Pugliese, *Biometrics: Bodies, technologies, biopolitics*, London/New York, Routledge, 2010; Rygiel 2011; Irma van der Ploeg, “Biometrics and the body as information: Normative issues in the socio-technical coding of the body”, in: David Lyon (ed.), *Surveillance as social sorting: Privacy, risk, and automated discrimination*, London, Routledge, 2002, pp. 57–73; Btihaj Ajana, *Governing through biometrics: The biopolitics of identity*, Basingstoke, Palgrave Macmillan, 2013; Keith Breckenridge, *Biometric State. The global politics of identification and surveillance in South Africa, 1850 to the Present*, Cambridge, Cambridge University Press, 2014; and others.

context marked by the persistence of problematic assumptions about difference. [...] Given the context for which they were developed, it is unsurprising that biometric technologies are imagined as able to definitively identify suspect bodies.”⁵⁶

As a 2003 report by the SANS Institute⁵⁷ on biometric scanning technologies pointed out, that technology is developed with a white Western body in mind and that this built-in whiteness causes difficulties for “darker skinned” people to be enrolled and verified in the system:

“Lighting conditions, which cause an image to be underexposed or overexposed, can cause challenges. Additionally, users with a darker skin tone can be difficult to acquire. Select Hispanic, black and Asian individuals can be more difficult to enroll and verify in some facial-scan systems because acquisition devices are not always optimized to acquire darker faces.”⁵⁸

Pugliese examined the intersection between biometric technology, bodies and race and found that biometric technologies are “infrastructurally calibrated to whiteness – that is, whiteness is configured as the universal gauge that determines the technical settings and parameters for the visual imaging and capture of a project”⁵⁹. As Richard Dyer analysed in his book *White* in 1997: “The apparatus (photographic media) was developed with white people in mind and habitual use and instruction continue in the same vein, so much so that photographing non-white people is typically constructed as a problem”⁶⁰. Unacknowledged, racialized and gendered coordinates “determine the discursive infrastructure of particular biometric systems”⁶¹.

An effect of the built-in ‘whiteness’ of the technology⁶² is that non-white people will bear a disproportional share of ‘failures’ in the system, which activates manual and/or extra control, for example, at the border. This is a situation that will perhaps mimic the current situation of manual profiling by border guards, when non-white persons seem to be selected disproportionately for extra checks. However, in continuation of

⁵⁶ Magnet 2011, p. 50.

⁵⁷ SANS Institute presents itself as a cooperative research and education organization, providing computer security training and information security research.

⁵⁸ SANS Institute, “Biometric Scanning Technologies: Finger, Facial and Retinal Scanning”, *SANS Institute. InfoSec Reading Room*, 2003. Available at: <https://www.sans.org/reading-room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning-1177> [accessed June 21, 2017].

⁵⁹ Pugliese 2010, p. 62.

⁶⁰ Richard Dyer, *White: Essays on race and culture*, London/New York, Routledge, 1997, p. 89.

⁶¹ Pugliese 2010, p. 114.

⁶² Facial recognition can be understood in continuation of Dyer’s analysis of on camera and photo technology analysed by Dyer for the built-in white bias.

the widespread imagined technological neutrality, the profiling and targeting of non-white persons will now appear disguised through technology as objective and non-discriminatory. This contradicts the EU Commission's claim that biometric technology will reduce discrimination and racial profiling and also highlights the significance of "automated decision-making" in biometric systems.⁶³ The lack of transparency behind the algorithms which determine decisions underpins the fiction of objectivity and a lack of discrimination in the systems. It also blurs the effect of producing 'statistical discrimination' through data mining.

The focus on the particular kind of governmental technology is exactly this; the technified "gaze of the governor"⁶⁴, tracking and scanning through enormous amounts of data to identify the specific, bodily differences that single you out as an object for surveillance and control, and at the same time subjectify the human being as a container of a physical, essential and unique identity. Essential identities are constructed in the fabric of the biometric systems through technique, algorithms, data-mining, profiling etc. as materialised social categorisations of gender, class, ethnicity, sexuality etc. You could say that the paradigm of the biometric system is more of a "scan-opticon"⁶⁵ with the capacity to manage populations through bodily identification and with a spatial flexibility to create zones, gates and borders anywhere.

CONCLUSION

Tightening up controls will likely increase the number of migrants being detained and deported, making residence more difficult. Biometric surveillance and profiling, separate the privileged from the unprivileged, the desired from the unwanted, the non-deportable from the deportable. It is an ongoing development, which is also linked to the ambition of enumeration and surveying irregular migrants.

We can trace a development going from governing humans with documents to governing bodies captured by birth and geography and having the global geometry of power laid down in fingerprints, facial and iris scans, DNA. This also indicates a possible transformation of the political rationality of problematising 'illegal migrants' to problema-

⁶³ Cp. Bigo et al. 2012.

⁶⁴ Rose 1999.

⁶⁵ Helle Stenum, "Biometric citizenship and alienage: new and re-structuring technology of government of mobility?" Paper presented at the conference: Reconfiguring borders and mobility in times of crisis, September, 26-28, Danish Institute for International Studies, 2012. Available at: [http://forskning.ruc.dk/site/da/publications/biometric-citizenship-and-alienage\(1c5b48bf-2510-412e-bf56-5164c4b4f89a\).html](http://forskning.ruc.dk/site/da/publications/biometric-citizenship-and-alienage(1c5b48bf-2510-412e-bf56-5164c4b4f89a).html) [accessed June 20, 2017].

tising ‘illegal bodies’. Migrants will, however, likely strategise to overcome the new technological regime.

Despite significant differences in the way biometrics is used as a technology to govern non-citizens and anti-citizens on the one side, and citizens on the other, biometric technology is an invasive device of government. It is now also the foundation for governing citizens by means of what Agamben has called the “bio-political tattoo”⁶⁶. In 2004, he cancelled a guest lecture in the US because he did not want to submit himself to having his fingerprints taken at the border:

“The bio-political tattoo imposed upon us today when we want to travel into the United States is the baton of what we might accept tomorrow as the normal way of registering into the mechanism and the transmission of the state if we want to be identified as good citizens”⁶⁷.

While Agamben had the capacity to control his fingerprints being taken back in 2004, who has the capacity to control who takes, or tags our facial images now?

⁶⁶ Giorgio Agamben, “Bodies without words: Against the biopolitical tattoo”, *German Law Journal*, 5 (2), 2004, pp. 168–169.

⁶⁷ Agamben 2004, p. 169.