SOURCE | Societal Security Network

VIRTUAL CENTRE OF EXCELLENCE FOR RESEARCH SUPPORT AND COORDINATION ON SOCIETAL SECURITY

# D6.2

# SOCIETAL ETHICS

# AND

# BIOMETRIC TECHNOLOGIES

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313288.

# D6.2 Report on Societal Ethics and Biometric Technologies

**Abstract:** This report addresses the widespread ethical issues raised by the increasing use of biometric technologies. It concentrates on the social and political effects of novel governmental schemes of policing, surveillance and identity management that combine biometric information with cloud based computing and the automated analysis of big data. In doing so, the report aims in particular to analyse the implicit value assumptions in the deployment of biometric technologies and the legal and rights issues these are raising. To date, ethical analyses of biometric technologies have tended to focus on the impact on individuals, with an emphasis on privacy. This report complements this focus by highlighting societal dimensions of the ethics of biometric technologies.

**Contractual delivery date:** 36

**Actual delivery date:** 36

**Version:** Final

**Total Number of pages:** 50

**Author:** Nina Boy, Elida Jacobsen and Kristoffer Lidén

**Reviewers:** Emma Mc Cluskey and Klaudia Tani

**Dissemination level:** PU

**Version Log**

| Issue Date | Rev. No. | Author | Change |
|---|---|---|---|
| 06.12.16 | 0.1 | Nina Boy et al | Full draft for review |
| 31.12.16 | 0.2 | Nina Boy et al | Final |

Deliverable submitted 31.12.2016 (M36) in fulfilment of requirements of the FP7 project, SOURCE – Virtual Centre of excellence for research support and coordination on societal security (SEC-2012.7.4-2: Networking of researchers for a high level multi-organisational and cross-border collaboration)

# Contents

Introduction ..... 4
1. The pros and cons of biometric technologies ..... 7
1.1. Definitions ..... 7
1.2. Biometric benefits ..... 8
1.2.1. The promise of security in a networked society ..... 8
1.2.2. The promise of global development and shared prosperity ..... 10
1.3. Critical voices ..... 12
1.3.1. Function creep ..... 12
1.3.2. Reliability and accountability ..... 14
1.3.3. Human identity ..... 15
1.3.4. Biocapitalism and biosurveillance ..... 16
1.4. Summary ..... 17
2. Fingerprinting Europe: the irresistible rise of the biometric ..... 18
2.1. Refugee management ..... 18
2.2. The '9/11' effect ..... 18
2.3. Database states ..... 20
2.4. Smart borders ..... 20
2.5. Summary ..... 22
3. Transforming social institutions ..... 24
3.1. Biometric technologies and the interactions they produce ..... 24
3.2. Case studies ..... 26
3.3.1. Counter terrorism and policing: facial recognition in the UK ..... 26
3.3.2. Asylum and refugee registration in Europe: EURODAC ..... 28
3.3.3. India's biometric scheme: national IDs for multiple purpose ..... 29
3.3. Summary ..... 30
4. Impact on non-technical bonds of community ..... 31
4.1. Coded communication ..... 31
4.2. Open bodies ..... 31
4.3. End of the social? ..... 32
4.4. End of the state? ..... 33
4.5. Summary ..... 34
Conclusion ..... 35
References ..... 38
Suggestions for further reading ..... 44

## Introduction

Biometric technologies are rapidly becoming integral to the governance of populations world-wide. Identification and verification practices are taking place in as disperse contexts as border checkpoints and asylum processes, welfare programs, spaces of humanitarian relief, policing and counter-terrorism practices, banking, elections and commercial transactions. India today hosts the world's largest biometric database, numbering biometric data of more than 1 billion residents based on finger printing and iris scanning. The database is a foundation for citizen-wide verification purposes, and is emerging as the main foundation – Aadhaar – for service delivery of the state. It is expected that similar forms of biometric usage and large scale databases will increasingly become the main means of states to identify citizens and non-citizens.

In some countries biometric registration is also made compulsory. In September 2016, the Gulf state Kuwait announced an investment of 400 million USD into the creation of a nation-wide biometric database, in response to a terrorist attack by the IS in 2015. Kuwait is the first country in the world to have introduced a law calling for the compulsory DNA testing of all its citizens, as well as all visitors, whatever their reason for entering the country. Those refusing to give a sample face a one-year prison sentence and a fine. In an open letter, the European Society of Human Genetics joined the UN Human rights panel in stating serious concerns with the impact of the law on the right to privacy and deemed the law a potential cause for discriminations, based for example on making citizenship dependent on genetic ancestry.

The examples of India and Kuwait represent the most extreme cases of the large-scale application of biometrics in the name of the security and welfare of society. Even in voluntary, or seemingly voluntary, uses of the technology, profound ethical questions arise. These include issues of human dignity and identity (individuality) and basic rights such as privacy, autonomy, bodily integrity, confidentiality, equity and, in the case of criminal investigation, due process (Irish ethics report 2009: vi). In addition to such impact on individuals, biometric schemes also affect societal bonds and cohesion, as well as political order. This is the societal dimension of the ethics of biometric technologies, defining the scope of this report.

In Europe and the US, there are strong legal restrictions on the collection and processing of biometric data. In particular, concerns for privacy and data protection have been instrumental in hampering new uses in spite of dramatic technological advances. There is a range of commercial uses subject to the consent of the users, in particular systems for access control based on finger prints, iris scans and more. Public applications are generally limited to passports/national IDs, the registration of migrants (finger print, portrait/facial recognition) and criminal forensics (finger print, DNA, face recognition, voice recognition, gait recognition). However, new systems of integrating biometric databases in police work are being introduced across Europe, for instance for controlling people's identity with handheld devices and automated recognition on video cameras (CCTV). These uses are controversial, but find strong support in their relevance for surveillance and counterterrorism.

Security concerns are particularly salient for the use of biometric technologies, because exceptions to rules of privacy and data protection are made when 'national security' is at stake.[1] Terrorism is usually defined as a threat to national security. With the increased scope of counterterrorism, encompassing 'radicalization' of citizens as well as immigration and the return of foreign fighters, the potential uses of biometrics for the 'exceptional' protection of national security is vast. It has already opened for advanced biometric technologies of identity management and surveillance by states of their own citizens that were inconceivable just a few decades ago. Meanwhile, we see a broadening of the security concept, encompassing 'new' concerns like pandemics and natural disasters. These fields present us with new potential uses of biometric technologies for crisis management, and the connection to the security of society makes a case for their legality.

A similar development is seen in the field of humanitarian assistance, where the security rationale of protecting lives intuitively trumps considerations of privacy and data protection. Often, these operations take place in countries without elaborate data protection regulations, in addition to involving a state of emergency similar to concerns for national security. Humanitarian organizations utilizing biometrics for identification purposes, for instance in connection with food and cash distribution, are increasingly aware of the data protection concerns that follow. Yet, as outlined in Chapter 1, there are strong incentives for further expanding the uses, integrating them with the analysis of big data and crowd sourcing for more efficient humanitarian programming.

In general, the potential for sharing biometric data on web-based servers, as well as combining these data with other data for the sake of public and commercial service delivery are changing the political and economic significance of biometrics. At the broadest level of prospective uses, biometric technologies are highly relevant when societies 'go digital'.[2] The more of our lives that move to the digital sphere – including welfare provision, voting and contractual agreements – the more important trustworthy sources of identification become.

In order to devise political responses to these developments, it is essential to understand their perils and promises. Are for instance current legal regulations in accordance with their underlying ethical premises? Is EU data protection law too restrictive, hindering essential innovation and rationalization? Or do concerns of privacy and data protection withstand arguments for the promises of biometric applications in new systems of governance and commerce? How does the broadening of security politics from 'national' to 'societal' security affect this picture? Central to such analyses is the security of the biometric data themselves. Biometrics provide essential solutions to problems of cyber security, like identity theft. Paradoxically, the theft of biometric data is itself a serious concern that might grow exponentially with the expanding uses of biometric security solutions.

Before answers to such questions can be devised, a series of distinctions must be made. Firstly, between different kinds of technologies, their application and their social and political contexts. Second, between different types of arguments and their ethical presuppositions. So far, ethical considerations of biometrics have highlighted the consequences of biometrics for the privacy,

[1] At the level of EU data protection regulation, this category of potential exemptions and restrictions is specified more broadly as public security, defence, national security and criminal law. See e.g. EU Data Protection Directive 95/46/EC Section 6, Article 13 (1); and EU Directive 2016/680, par. 14 and Art. 16 (4).
[2] See e.g. the case on Estonia in Chapter 3 of this report.

autonomy, welfare and security of individuals. In this report, we concentrate on the social and political dimensions of these concerns, as aspects of the *societal* ethics of biometric technologies. While relating to the broader range of applications mentioned above, the scope of the report is biometric technologies in the field of security politics broadly defined – as delimited by the notion of societal security.[3] The report draws on examples from around the world of relevance to the legal regulation of biometrics in Europe in particular.

Evidently, the effects of biometrics at the individual and societal levels are closely connected. Highlighting the societal dimension in this report is a response to the individual centric focus of previous studies. This is not an argument for shifting the focus away from the individual but to include the societal dimension in future studies. As such, this report is an exploratory thematic study of the societal dimension. Far from exhausting the issue, it suggests arguments and perspectives to consider in the evaluation of concrete technologies and policies.

In section 1, the meanings and modes of biometric technology are introduced. A set of established narratives on the benefits and costs of biometrics are then presented. Section 2 relates the topic to the scene of European politics and legislation by providing an overview of the introduction of biometric schemes of refugee management, national ID and policing in the European Union. A set of controversies and dilemmas are identified that relate to the societal impact of the schemes. Against this conceptual and political background, section 3 presents three cases of how social institutions are affected by large-scale biometric schemes of public governance. Section 4 outlines a range of broader societal perspectives that ought to be considered when regulating new applications of biometrics. In the conclusion, the argument of the report is summed up and a set of issues for further consideration are suggested. The report ends with a list of suggestions for further reading.

Research for this report has been carried out within the SOURCE Societal Security Network, as part of Work Package 6: Ethics, Law and Human Rights.[4] The objective of the work package is to provide the documentary and analytic foundations for on-going research on the dependencies between societal security and ethical values, in particular in comparison with values implicit in 'hard' security measures. The report is written in continuation of Report D6.1 on the role of values in European threat analyses and security strategies.[5] Further material from the SOURCE project and other references on societal security, ethics and biometrics can be found in the 'Knowledge base' of SOURCE: http://societalsecurity.net/knowledgebase.

[3] ISO Standard 22300:2012 defines *societal security* as: 'protection of society from, and response to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards, and technical failures.' On the concept of societal security, see SOURCE deliverables 1.1: Inception report, pp. 2-7; 4.1: Report on theory and methodology for mapping of societal security networks, pp. 3-14; and 6.1: Report on human values in threat analysis, pp. 8-11. Available at: http://www.societalsecurity.net/content/source-deliverables.

[4] For information on the SOURCE project, see http://societalsecurity.net/.

[5] Available at: http://societalsecurity.net/sites/default/files/imce/d6.1_values_in_threat_analysis.pdf

# 1. The pros and cons of biometric technologies

## 1.1. Definitions

The term 'biometrics' is derived from the Greek words 'bio' meaning life and 'metric' meaning to measure, and refers to the application of statistical analysis to biological data. In the context of security, the most directly relevant biometric technologies are those employed for the purpose of personal identification. As Mordini and Massari (2008: 489) note, any biological or behavioural characteristic may function as a biometric identifier as long as it satisfies four basic requirements: 1) *collectability* (the element can be measured); 2) *universality* (the element exists in all persons); 3) *unicity* (the element must be distinctive to each person); 4) *permanence* (the property of the element is permanent over time). For almost a century only fingerprints have satisfied all these conditions. Current biometric technologies – so-called first generation biometrics – now include ultrasound fingerprinting, iris scans, hand geometry, facial recognition, ear shape, signature dynamics, voice recognition, computer keystroke dynamics, skin patterns, foot dynamics, DNA as well as full body scanning.

Future biometrics – the second generation of biometrics – are expected to extend identifiers to neural wave analysis, skin luminescence, remote iris scan, advanced facial recognition, body odour, vein recognition and more (for background literature on some of these various techniques and their legal ramifications, see 'Suggestions for further reading'). Beyond the extension of identifiers, future biometric identification is moving towards *multimodal* systems that match different identification technologies, as well as *multiple* biometric systems that combine different identifiers. Behavioural biometrics – measuring behavioural characteristics such as signature, voice, keystroke pattern, gesture recognition and gait – are also gaining in importance (ibid., see also UK House of Commons 2015).

Biometrics have a long history of use in prisons and in the colonial periphery (Pugliese 2010) as well as in criminal identification. The digitalization and automation of biometric recognition processes has however led to a dramatic evolution of the technology and its possible uses. Digital biometrics differ from traditional biometrics both *quantitatively* (the digit format allows us to collect, store and process electronically a huge amount of data in a short period of time) and *qualitatively* (being numeric strings instead of icons, digital representations have different qualities from analogical representations) (Mordini and Massari 2008: 489). Digitalization has generally expanded the class of automatic identification technologies (Auto-ID), that is, technologies that collect and identify data without human involvement. These include Bar Codes, Optical Memory Cards, Contact Memory buttons, Radio Frequency Identification, Radio Frequency Data Capture, Micro Electro Mechanical, Systems, and Smart Cards (ibid: 488). But in contrast to Auto-ID devices identifying items, biometrics can only be used to recognize living beings (animals and humans).

Biometric systems operate in three key steps. The subject is first captured by a biometric imaging system that focuses on that portion of a physical feature that is time-invariant within some statistical limit. The image is then digitally converted through the use of algorithms into a template that is stored in a database in the system. When the subject presents itself again to the biometric system, the 'live' digital image of a body part is matched against the previously recorded and stored image of the same part. More specifically the process of identification entails two aspects: *verification*, that is, a one-to-

one comparison to authenticate an individual's identity; and *identification,* that is, a one-to-many comparison where the individual's template is matched against all the templates in a given database (Irish ethics report 2009: 3). A modern biometric identification system usually consists of six modules: sensors, aliveness detection, quality checker, feature-generator, matcher, and decision modules (Mordini and Massari 2008: 491).

Historically, individuals have been identified by legal names, locations, tokens, pseudonyms and other features (ibid: 488). Even fingerprints have been used at least since 7000-6000 BC by the ancient Assyrians and Chinese as a form of identification to indicate or authenticate the authorship of a document or a work of pottery (O'Gorman 1999: 44). But it was only in the modern age that identification was seen as a general social problem (Garfinkel 2000, in Aas 2006). Establishing stable identities of their subjects and national identification systems was one of the central tasks of modern states (Torpey, 2000; Lyon 2001). With the advent of the internet, the significance of identification gained a new dimension in the protection of personalized access to accounts. In these contexts, identification and verification involve the use of a password, personal identification number (PIN) or cryptographic key ('something you know') or the possession of an identity (ID) card, smart card or token ('something you have') (Jain *et al* 1999: 14-15). Where passwords and passports can be forgotten or stolen, a biometric trait is part of an individual and as such it offers 'the third element of proof of identity, i.e. 'something you are''(ibid: 14-15). As Mordini and Massari (2008: 450) conclude: 'Complex personal recognition schemes, tattoos, seals, passports, badges, safe-conducts, passes, passwords, PINs: biometrics make obsolete […] these traditional identification paraphernalia and – at least in the long run – promises to replace all of them.'

As the introductory example illustrates, there is an ongoing interest in utilizing DNA typing methods for biometric purposes. Conventional uses range from disaster victim identification and family unification to paternity tests and criminal forensics. Forensic DNA testing has served as investigative resource in the criminal justice system since the 1990s: the European Council recommended the use of DNA in European policies and legislation relating to criminal justice in 1992[6]; in the US criminal justice system DNA testing has been in use since 1998. The collection and storage of DNA profiles in a database enables the systematic comparison and automated matching of crime scene samples with individual profiles. Current efforts concentrate on decreasing the time required to perform a DNA test and integrate the extraction, amplification, separation and detection processes for forensic DNA without human intervention. Rapid DNA testing reduces the time-span required from two days to under two hours and, aside from the criminal justice system, widens the use of DNA as biometric mode to the areas of immigration, airport and border security, military intelligence and mass fatalities.[7]

## 1.2. Biometric benefits

### *1.2.1. The promise of security in a networked society*

Biometric applications are expanding fast in sectors as different as border security, access control, surveillance, law enforcement, national ID, financial services and payment systems, humanitarian aid

[6] See https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4513018/
[7] See https://www.nist.gov/programs-projects/dna-biometrics

and workforce management. The apparent disparity of these different applications becomes clearer when considered in the context of the liberal security paradigm of securing circulation (see Section 2 of SOURCE Report D5.1, Boy 2015). Security in a globalized world is concerned with the problems posed by interdependencies and flows rather than with problems posed by demarcations between internal and external affairs. The task of seeking to separate 'good' circulation (business travel, trade, tourism, skilled workers) from 'bad' circulation (terrorists, viruses, toxic assets, unwanted immigrants etc) vastly increases the need of identification. As Lebovic (2015: 844) notes, 'biometrics as a system [is] meant to offer a quick, neutral, efficient, and reliable way to recognize people in movement'. In the present world of increasing global flows of people, the 'state's task of giving stable identities to mobile and versatile populations becomes extremely difficult, if not impossible' (Aas 2006: 146), explaining both the appeal of biometric ID as well as what has been termed a 'securitization of identity' (Muller 2004). Biometrics provides the information by which to distinguish legitimate from illegitimate circulation and thus presents itself as 'a smart scientific solution of managing risk without impeding circulation' (Amoore 2006: 339). The former Secretary of US Homeland Security, Tom Ridge, in this sense has praised biometrics as a 'great tool that helps move low risk travellers more efficiently so that resources can be focused elsewhere, where the need is greater' (Homeland Security 2005: 1, in Amoore 2006: 342). Biometric technologies have received a boost in security efforts post-9/11 and become a core feature of the war against terror (Amoore 2006). Fingerprints and facial recognition were seen to be largely responsible for the quick identification and capture of the New York City terror bomber Ahmad Khan Rahami[8], an example of the operative use of biometrics to identify, track and apprehend terrorists.

The unprecedented accuracy and certainty of identification and the improvements in efficiency and speed make biometrics seem the only means of identification fit for security in the digital age. With the increasing demand for identification, one of the main arguments put forward in favour of biometric identification has been the apparent fool proof nature of identification. Earlier ID systems such as passports, home address, social security number, or forms of automatic ID that represent technological versions of older forms (eg smart tags, RFIDs), entailed certain details deemed necessary to associate individuals to identities. These forms thus are 'not true proof of identity, (but) rather statements as to who a person claims to be' (Mordini and Massari 2008: 489). By contrast, automatic biometrics shift verification from verifying a relation between an individual and a document to a relation between an individual and itself, i.e. they induce a shift from *indexical* data to *biocentric* data. As Alterman (2003: 144) notes: 'Indexical data has no internal relation to an embodied person' and requires positive identification by some other method as 'information is only contingently tied to a particular individual'. Biocentric identification on the other hand is based on the body as *natural* passwords or identity cards (Aas 2006: 145), entailing not a contingent but a necessary relation of identity. While the misuses of ID may threaten the integrity of the system, biometric identification encompasses intrinsic identity fraud prevention. Securing circulation in the digital age thus is beginning to found itself on the body as new source of certainty.

[8] See http://www.biometricupdate.com/201609/the-need-for-dialogue-biometrics-are-good

### *1.2.2. The promise of global development and shared prosperity*

The second major argument put forward for biometric identification is its utility in the context of global development and emergency management. International organisations are promoting biometrics as a clear asset in the fight against poverty and for emergency relief, and a central factor in achieving the global sustainable development goals (SDGs) of the 2030 Agenda for Sustainable Development. According to the World Bank, around 2.4 billion people currently do not possess an official, government issued and recognized document as proof of their legal identity.[9] As Mordini and Massari (2008: 490) argue, biometric ID could 'contribute to give a face to the multitude of faceless people in developing countries, contributing to turn these anonymous, dispersed, powerless, crowds into new global citizens.' The World Bank in 2014 launched the initiative ID4D (Identity for Development), which seeks to facilitate access to services and rights for all by means of 'identification systems using 21st century solutions'. The target of universal identity is seen as a core enabler for five distinct further SDGs: 1) *Financial inclusion*: Access to financial services for approximately 375 million unbanked adults in developing countries. 2) *Gender equality*: Proof of legal identity will enable women to better assert their rights and have greater say in household decisions. 3) *Access to health services*: identifying beneficiaries will allow countries to better manage health interventions; 4) *Social safety net:* bringing social assistance to over 875 million people living in extreme poverty and 5) *Improved governance*: enabling governments to increase the accountability of government institutions and curb fraud and corruption. In 2015 the World bank co-authored a report with the consultancy firm Accenture to advise developing nations on how to create universal ID management systems regardless of their country's level of technological infrastructure. According to this narrative, biometrics thus carries the promise of leap-frogging over decades if not centuries of lagging development (see the case study of India's biometric database in section 3.3.3).

The UN has also incorporated biometric identification into its humanitarian assistance to refugees to improve the 'timeliness and intelligence of humanitarian response' (Duffield 2015: 88) and to eliminate fraud.[10] The earliest use goes back to the 2000s where iris recognition was employed for the repatriation of refugees from Pakistan back to Afghanistan and fingerprints technology served to identify refugees in camps in Tanzania and Kenya and at various sites in South Sudan (Lindskov Jacobsen 2015: 160-61). Andrew Harper of the United Nations High Commissioner for Refugees (UNHCR) states that the iris recognition technology used as part of the UN's assistance to Syrian refugees across the Middle East has significantly improved efforts in distributing 120 million USD in aid to nearly two million refugees. According to Harper, the benefits are both economic gains in efficiency as well as the protection of human dignity: 'Refugees don't have to come to us, they can just go to a bank fitted with iris scanning, so we've not had to deploy any staff for procurement, transportation or warehousing… We are able to give refugees the money at the time of their choosing and they can use it for the reasons they believe they are most important. It reinforces the dignity of the refugee, and human dignity is the basis of almost everything we do. We have more money to help people that are most in need'.[11] Since 2013 biometrics have reduced the overhead for the refugee program from nearly

[9] See http://blogs.worldbank.org/voices/finding-missing-millions-can-help-achieve-sustainable-development-goals
[10] See http://www.ibtimes.co.uk/un-biometric-iris-scanners-transforming-syrian-refugee-programme-by-preventing-fraud-1527362
[11] See http://www.biometricupdate.com/tag/united-nations

20% to approximately 2%[12]. Through REACH, a consortium of data NGOs and UN satellite and training agencies, UNHCR is in the process of integrating satellite imagery, interactive mapping, biometric fingerprinting and text messaging into an integrated refugee management tool (Duffield 2015: 87, Jlevy 2013). Other UN-supported initiatives include biometrics to help anti-piracy efforts in Somalia, the verification of voters in Kenya, Uganda, Zimbabwe, Pakistan to boost credibility of presidential, legislative and local elections, the expanded use of advance passenger information to prevent terrorism and assistance with the preliminary stages of India's national biometric project (cf. Jacobsen 2012).[13]

If these two arguments for biometric identification appear distinct, it is clear that biotechnology is increasingly merging security, humanitarian and economic concerns into one nexus. The UNHCR decided to deploy IrisGuard portable iris-scanners after seeing how these were successfully used in banks, ATMs, and airports across the Middle East. The UN iris readers have in turn played a key role in integrating more than 80 percent of refugees residing outside of camps into the existing banking system.[14] The security benefits of biometrics recognized by the UN include the ability to follow migrants from one camp to another, ensuring that members of extremist groups are unable to misrepresent themselves, and preventing cards containing aid money from being stolen and resold. The 'growing fusion of security, information, and identification systems' (Lebovic 2015: 844) is actively promoted in the development of applications that coordinate different government functions: The programme Nexus 7, developed by MITRE corporation, integrates reality mining, dynamic network analysis, behavioural modelling and advanced simulation techniques with biometric database management, village surveys and checkpoint intelligence. Using a wide range of developmental data, including changing wage rates and commodity prices, Nexus 7 constitutes an all-encompassing attempt to 'quantify, model and predict the human, social, cultural and behavioural dimension of conflict' (Duffield 2015: 89). The 'digital development-security nexus' (ibid: 82) manifests in a cyber-infrastructure of integrated geospatial, biometric, demographic and mobile databases, sometimes supported by satellite remote sensing (ibid: 88). Yet the fusion of governmental tasks is not limited to developmental settings: The software suite MorphoCivis draws on fingerprint, portrait or iris separately and in combination for ID, to allow governments to define, store and manage the identity and individual rights of their citizens as one integrated function, including ID cards, passports, driver's license, health and welfare, visas and voting. The software also has a component to manage the interaction with the public.[15] Biometric identification is thus seen as technology with the potential to synthesize and optimise government functions generally in increasingly networked and digitalised societies as well as in humanitarian and developmental contexts.

[12] After the U.N. began implementing iris scanning for Iraqi refugees, the number of refugees asking for aid dropped by 30 percent in this region. Harper attributes this sharp decline to fraud reduction.
[13] http://www.biometricupdate.com/tag/united-nations. Over 14 million Kenyans were biometrically registered in the run-up to the 2013 election (Duffield 2015: 83)
[14] http://www.biometricupdate.com/201511/un-using-irisguard-iris-recognition-devices-to-aid-syrian-refugees-across-middle-east
[15] http://usa.morpho.com/civil-identity/biometric-data-management/morphocivistm

## 1.3. Critical voices

### *1.3.1. Function creep*

A primary concern with biometric technologies is the use, or abuse, of the technology and/or data with unintended consequences or for unintended purposes. Here the shift from indexical to biocentric identification noted above has implications for the nature of abuse: 'Where stolen passports are primarily an attack on one's property rights, the abuse of biocentric data represents an attack on […] one's sense of self' (Alterman 2003: 144). Biometric technologies form a kind of 'body language' and their perceived infallibility is founded in the specific quality of the body of 'speaking' quite independently of our conscious will' (Mordini and Massari 2008: 493). The body communicates even when the mind does not want to (Aas 2006: 154). While seemingly less intrusive than a body search at the airport, biometric ID opens up secrets of the body in radically different ways (Aas 2006: 145). The potential of abuse is increased by the fact that biometric systems tend to capture more data than strictly needed for identification. As Mordini and Massari note,

> *'Sensors unavoidably generate data about time and location, say, when and where the sample was captured. They may also collect shadow information, for instance any system for facial recognition inescapably ends up collecting extra information on people's age, gender and ethnicity, and – given that facial expressions are topological configurations that can be measured – they have also the potential to detect people's emotional states, as reflected in their expressions.'* (2008: 491)

Sensors may thus elicit data on the medical history of the identifying person, for example by detecting anomalies such as eye diseases that prevent initial enrolment in the system. They also invite the comparison of specific details over time at enrolment and subsequent entries, allowing for patterns to be analysed not much different from medical diagnosis (2008: 492). Thus biometric data 'could become a covert source for prospective medical information, allowing people to be profiled according to their current and potential health status' (2008: 492-493). DNA analysis even more explicitly has the potential to reveal what may happen in the future. The more mature biometrics become, the more intrusive (2008: 494), and there is a concern that the generated 'data surplus sooner or later becomes available for unintended or unauthorized purposes' (491).

Contrary to public belief, Mordini and Massari hold that biometric information is less prone to misuse once the captured features have been digitalised, precisely because the purpose of the template is the efficient storage of identifying data that discards any unnecessary data (2008: 492). It is impossible to 'deduce original biological and behavioural characteristics of an individual from a template' and engage in template reverse engineering. Yet this impossibility depends on refraining from storing compressed biometric samples in the system or in the template. Template encryption is further necessary to reduce the risks of identity theft, data mining and profiling. As the US National Research Council cautions,

> *'even a biometric system that does not internally link an individual's biometric data with other identifying information may fail to preserve anonymity if it were to be linked using biometric data to another system that does connect biometric data to identity data. This means that even*

> *a well-designed biometric system with significant privacy and security protections may still compromise privacy when considered in a larger context' (2010: 92).*

In the context of the above-mentioned trend of integrating government functions both in the 'global North' and the 'global South' the risk of personal records being linked across systems and of function creep increases also since the logics and imperatives underpinning security and the perceived gains from integrating databases tend to dominate concerns about their adverse effects. The more embedded biometric technologies become in the synchronisation of government functions ranging from development to emergency management to humanitarian assistance, the more fluid the exceptional logic of security may be integrated into a general model of social control. Where privacy restrictions and other legal safeguards provide some protection against function creep in the global-North[16], this fusion is more pronounced in the global-South. In the sombre assessment of Duffield, the global South is treated as a 'relatively open laboratory for developing the intelligence potential of (biometric) technologies […] often justified on the grounds that poor people and disaster victims are not bothered by privacy issues' (2015: 83). In addition to mapping and database management, for example, the UN consortium REACH in South Sudan also uses data-mining techniques to analyse the social dynamics and resource usage of the refugee camps. As Duffield submits,

> *'Once one begins to map, model and predict sociocultural organization and environmental pinch points among surveillant populations, a self-proclaimed development and humanitarian intelligence simultaneously and irrevocably blurs into security intelligence'* (2015: 88).

The US Social Radar tool, a data-mining programme developed to 'penetrate' the 'hearts and minds of a target population' and informed by a vast array of data sources including Facebook timelines, socio-metrics, political polls, spy drone feeds, aid agency reports and more, 'brings together within a single computer program, depending on the intelligence uncovered, the choice of either a timely humanitarian response or, alternatively, a whole-of-government security response… including the authorization of a drone signature kill' (Zenko 2012, in Duffield 2015: 90). Even in the global North, privacy concerns are increasingly on the defense against security rationales. In 2016 the US FBI proposed to exempt its biometric database launched in 2008 known as the Next Generation Identification (NGI) System from certain provisions of the Privacy Act that require federal agencies to share with individuals the information they collect about them and that give people the legal right to determine the accuracy and fairness of how their personal information is collected and used. What has in particular been criticized is the combination of criminal and non-criminal information in the NGI database that includes data collected in a range of settings, including licensing of motor vehicles, volunteer and welfare screenings, employer's background checks and visa applications. As of December 2015, the NGI system contained 70,783,318 criminal records and 38,514,954 civil records.[17] The integration of government functions and databases at the least provides the preconditions for function creep, as will be further elaborated in section 3.

[16] According to the EU Data Protection Directive (art.7 par.1) no data collection can go unnoticed by the subject that is being monitored, except in the case of 'processing of data relating to offences, criminal convictions or security measures'. https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm

[17] See https://theintercept.com/2016/06/01/the-fbi-wants-to-exempt-massive-biometric-database-from-the-privacy-act/

Function creep is a common denominator for a wide range of phenomena that need to be analysed in their own right. First, there is function creep within the context that the technology is introduced within. This is the kind outlined above, where the technology may generate new uses and perversions. Second, function creep may result from a change in social or political context. This can be a shift of leadership, or reforms of the political system. Indeed, the emergence of serious political struggle between a government and the opposition present the authorities with strong incentives for appropriating biometric information from established schemes. For instance, access to personal data and technologies for the recognition of persons who try to operate anonymously 'under the radar' of the authorities is a powerful tool. This can be contexts of civil war or dictatorships, but also applies to situations of intense struggles in relatively democratic countries where the technology is used in order to manipulate political dynamics. Being perfectly suited for autocratic regimes, national biometric schemes may affect the very incentive structures for democratic government, entailing function creep. Finally, when technologies are introduced and legalized in democratic contexts and exported to, or replicated by, autocratic regimes, it necessarily involves the creeping of their original functions.

### *1.3.2. Reliability and accountability*

Biometric systems face two types of security challenges: they may be employed to secure access to another resource or system, but are also vulnerable to both unintentional and intentional technical failures in themselves. Despite the perceived infallibility of biometric identification, a report by the US National Research Foundation in 2010 states that biometric recognition systems contain an inevitable margin of error:

> *A biometric match represents not certain recognition but a probability of correct recognition, while a nonmatch represents a probability rather than a definitive conclusion that an individual is not known to the system. That is, some fraction of results from even the best-designed biometric system will be incorrect or indeterminate: both false matches and false nonmatches will occur. Moreover, assessing the validity of the match results, even given this inherent uncertainty, requires knowledge of the population of users who are presenting to the system—specifically, what proportions of those users should and should not match. Even very small probabilities of misrecognitions—the failure to recognize an enrolled individual or the recognition of one individual as another—can become operationally significant when an application is scaled to handle millions of recognition attempts* (NRC 2010: 4).

While in password- or token-based systems a breach can usually be remediated by issuing a new password or token, the breach of a biometric system may have far more serious consequences, since it is generally not possible to replace a biometric trait that has been compromised (2010: 6). As much as the irrevocable link between biometric traits and a persistent information record about a person (2010: 85) is held as a strength of biometric recognition systems, as severe may the damage be that is caused by an erroneous link. While the technology's error rate has significantly decreased from the early 1990s, documents obtained by EPIC revealed that the FBI was willing to accept a 20 percent error rate for its face recognition technology as of 2010 (FBI 2010). Studies have found that the error rate for face recognition systems increases logarithmically with the size of the dataset and that error rates are highest for groups that are overrepresented in the system, such as African-Americans in the

NGI database.[18] It is essential therefore that biometric systems are subject to human validation and auditing procedures, which significantly constrains remote or distributed applications. Automated verification is possible in some settings but does not substitute for human supervision where high degrees of confidence are required (NRC 2010: 7). Accountability of biometrics is often framed as improved user accountability, e.g. employee accountability through workforce management or a reduction of identity fraud in welfare systems. But this framing omits the 'accountability problem' of biometric systems themselves, and the often insufficient formal procedures for audit and mechanisms for complaints and redress (Irish Ethics Report 2009: 96). This is particularly pertinent when identifying subjects are in a vulnerable position when presenting to a biometric system: whether refugees, victims of natural catastrophe in need of humanitarian aid, or travellers at the airport looking to board their flight, if not outright compulsory, the 'voluntary' participation in biometric ID often marks a situation of captive demand, where the situation of the subject leaves no choice but to consent to biometric ID.

### *1.3.3. Human identity*

If the loss of control over personal data associated with function creep and the blurring lines of the purposes of biometric surveillance have primarily been taken up by privacy advocates and civil liberty organisations, there is a more philosophical concern with the impact of biometric technologies of identification on human 'essence' and identity. This impact has been discussed under the term of the *informatisation of the body* (van der Ploeg 2003, 2008) (the societal implications of this are discussed in section 4). As van der Ploeg (2008: 85) notes:

> *[T]he human body is co-defined by, and in co-evolution with, the technologies applied to it. [...] the dominant view of what the body is, what it is made of and how it functions, is determined and defined by the practices, technologies and knowledge production methods applied to it [...] Seen in this light, biometrics appear as a key technology in a contemporary redefinition of the body in terms of information*.

The informatisation of the body entails the 'digitalization of physical and behavioral attributes of a person and their distribution across the global information network' (Mordini and Massari 2008: 494). Rather than determining a pre-existing identity, biometric practices *establish* identity (van der Ploeg 1999: 154). Contrary to analogical representation, 'digital representations always imply a certain degree of simplification, which modifies the nature of the represented object' (Mordini and Massari 2008: 494. On the one hand, the positioning of the body as infallible source of identification elevates the body over the mind or person: biometric systems 'assume the necessary existence of a unique individual status and goal-oriented movement of its members in the community' (Lebovic 2015: 844) and thus establish the body as the means to control ambiguity, ambivalence and uncertainty (Amoore 2006: 338). On the other hand, the informatisation of the body has also been suggested to cause a process of *disembodiment* (Aas 2006). The electronic persona is seen as more representative – and in a sense more relevant – than flesh-and-blood bodies, engendering a move from the 'unity of body and mind, physical and social identity, to the unity of body and information as main truth' (2006: 153). This implies a shift from a personal to an individual truth: the connection of body to place grounded in

[18] https://theintercept.com/2016/06/01/the-fbi-wants-to-exempt-massive-biometric-database-from-the-privacy-act/

tradition is replaced by the connection of body to place grounded in traceable movements (cf. Lyon 2001: 74). Where on the one hand, the body serves as authenticating source for its data, it is on the other hand questioned whether biometric data constitute *authentic* human identification. The French National Consultative Ethics Committee for Health and Life Sciences in 2007 thus asks whether biometric data not in fact contribute to 'instrumentalizing the body and in a way dehumanizing it by reducing a person to an assortment of biometric measurements.'[19] As biometrics are concerned with (people in) movement, they 'do not care about the inside of the human, unless it assumes a bodily shape or – as the notion of character offered in the nineteenth century – told the operator something about its movement' (Lebovic 2015: 844). 'What the subject thinks, does or believes is irrelevant to what the institution controls; it is simply meaningless for the technological device' (Lianos 2003: 423). Biometric identification thus simultaneously heralds a move from citizens to pure biological ('bare') bodies (and from *bios* to *zoe*) (Agamben 1998) as well as the digital disembodiment and transformation of these bodies.

#### *1.3.4. Biocapitalism and biosurveillance*

For some observers, this dual movement is driven by a more profound and systemic shift in the generation of value. With genes increasingly defining personhood, recent developments in life sciences, biomedicine and biotechnology have been said to effect 'a wider reshaping of personhood along somatic lines and a mutation in conceptions of life itself' (Novas and Rose 2000: 485). As Cooper (2008) has illustrated, this politics of life is intimately connected with its economization, that is, a relocation of economic production at the genetic, microbial and cellular level. With the biotech revolution, life has been drawn into the circuits of value creation: At the very core of the new post-industrial economy is the transformation of biological life into surplus value (Cooper 2008). This constitutes a new phase of capitalism insofar as 'the environmental crisis, which signifies the end of growth, intersects with the promise of the 'regeneration of living futures' via the biological to 'create a new narrative that dispels capitalism's fears around limits' (Abergel and Magnusson 2014: 237). This implies an increasingly integrated logic of biocapitalism and biosurveillance, which is visible in the changing objective of *biosurveillance*. As Abergel and Magnusson (2014: 241) recount:

> *Originally, the term was used to describe a vast public health program, locally and globally coordinated to prevent and prepare in case of an epidemic such as the SARS outbreak, or against pathogenic agents and disease outbreaks, which affect our food system. More recently, especially in the wake of 9/11, the concept of biosurveillance has been extended to enclose and contain a series of newly identified potential risks outlined in new research programs and technoscientific orientations which have taken a decidedly biotechnological turn. These include the identification and containment, using an arsenal of technologies such as DNA tags, QR codes, RFID tags and biometric data, of illegal migrants and criminalized and marginalized people considered to represent varying degrees of threat.*

Advances in technology driven by the relocation of value creation to the biological also imply that civilian research projects in medicine and biology have the potential to be used in military applications

[19] French National Consultative Ethics Committee for Health and Life Sciences, 2007, Biometrics, Identifying Data and Human Rights. *OPINION N° 98.* Available at; http://www.ccne-ethique.fr/ docs/en/avis098.pdf

(dual-use research) including bioterrorism.[20] 'Biosecurity' both refers to measures to prevent dual-use biological materials from falling into the hands of malevolent parties as well as to preparedness in the event such contingencies. The expanding need to police 'biological threats' and the concomitant requirements for identification produce growing economic demand for innovative solutions by the biotech industry, while 'new ways of identifying threats and new pathologized identities … also generate new classes of risks that necessitate ever-increasing levels of surveillance' (ibid: 243). This circular logic reinforces both the appropriation of people as pure biological subjects and the production of biocapitalist innovations that 'mobilize(s) and modif(ies) vitality' (ibid: 245).

## 1.4. Summary

Biometric identification is seen as the primary means of providing security for networked societies in the digital age. In addition to their advantages for criminal forensics and commercial services, the apparent fraud-proof nature of biometric systems makes these superior to previous means of identification and allows to manage global mobilities without halting global flows. The benefits of biometric technologies for different government functions are promoted both in the 'global North' and the 'global South'. Critics point out that biometric systems are more vulnerable to function creep than previous forms of identification, as the generation of extra information derives from the very nature of the human body and does not depend on the consent of the subject. While the strong link between biometric feature and personal record is promoted as an asset by proponents of biometrics, it may also cause higher damage when the biometric system misperforms. Adequate auditing and redress procedures are therefore essential. The appropriateness and proportionality given the problem to be solved and the merits and risks of biometrics relative to other solutions need to be clearly communicated to the public. The potential of function creep increases with the synchronisation of government functions and databases. The emerging nexus of biosecurity, biotechnology and bioeconomy has been said to be driven by a relocation of value creation to the biological that profoundly affects the nature of human life: biometric systems thus effectuate an *informatisation of the body* as well as the digital disembodiment and transformation of these bodies. In sections 3 and 4, we consider how these changes affect the 'social and political body' as well.

[20] See e.g. https://en.wikipedia.org/wiki/Dual-use_technology

# 2. Fingerprinting Europe: the irresistible rise of the biometric

Before looking into the relevance of the narratives presented in section 1 for the consideration of social and political effects of biometric technologies, this section positions the study within the European legal and political landscape. It does so by concentrating on the regulation of uses of biometric technologies for refugee management, policing and counterterrorism in Europe. Centring on principles of data protection and privacy, recent developments in these regulations demonstrate the need for recognising the broader social and political effects of biometrics in government programs.

## 2.1. Refugee management

In 1998 a 'strategy paper' on EU migration policy issued by the Austrian presidency called for 'inducements' for developing countries to fingerprint their populations in case their nationals ever turned up undocumented in Europe (EU Council 1998). At the time, this idea was highly controversial.

Mandatory fingerprinting had long been seen as a way of implementing the 1990 'Dublin Convention' on responsibility for asylum applicants – under which the state of entry to the EU would be responsible for processing the asylum claim – but it would be five years before the 'EURODAC' database would be launched (see section 3.3.2.).

Under the Dublin/Eurodac rules, all asylum applicants and 'irregular migrants' are fingerprinted by the state in which they registered, allowing persons who then seek asylum in another state to be identified and returned to the EU state of first entry. During the latter stages of the EURODAC negotiations the EU member states agreed to reduce from 18 to 14 the age limit for inclusion in the database, prompting some debate about the age at which states should begin fingerprinting children. In May 2016 the European Commission proposed to lower the age limit from 14 to six, and to include facial images as well as fingerprints (European Commission 2016a). This is at least partly because asylum-seekers have been mutilating their fingerprints to avoid detection by member state authorities. Some member states have responded by detaining and/or penalising asylum-seekers for failing to provide fingerprints. There have been also been various calls from politicians for non-cooperative migrants and refugees to be sedated so their prints can be taken, coupled with reports that this is happening in practice.

Though EURODAC was established as an administrative tool for the purposes of determining responsibility for asylum applicants, access to the database was soon extended to law enforcement and security agencies to allow them to search for wanted persons. Under the latest proposals, they will be granted wider access still (ibid.).

## 2.2. The '9/11' effect

Biometric ID systems were much more widely promoted in the aftermath to 9/11. Just two weeks after the attacks in the USA, the German government proposed that 'each Member State should maintain centralised registers storing data on all third-country nationals present in the territory of the Union' and that there should be established 'a European central register' (EU Council 2001). At the time only Germany and Luxembourg even had so-called 'aliens' registers.

Three weeks later the Belgian presidency called for the automated collection and exchange of data on all visa holders. Following the hastily agreed USA PATRIOT Act, which introduced the requirement that all entrants to the US provide the authorities with biometric data upon arrival, the Benelux countries and Germany called for the inclusion of 'biometrics' in EU visas and residence permits (Statewatch 2003). Formal proposals were produced later in 2003, providing for the incorporation of digitised photographs, then fingerprints into the already harmonised EU/Schengen travel documents. In the event, it would be some years before all these proposals came to fruition, but ultimately all holders of EU travel documents would be biometrically profiled.

In 2003, the United States, supported by the EU, demanded an international agreement on biometrics using harmonised technical standards. This was quickly agreed at the International Civil Aviation Authority (ICAO, a UN body), which mandated digitised photographs (facial recognition) as the global standard for travel documents, with fingerprinting optional (ICAO 2003).

On the back of this agreement, the EU proposed in 2004 to introduce biometrics into EU passports (European Commission 2004: 116). The stated purpose of the proposal was to make passports harder to forge and establish a 'reliable link' between the holder and the document through the biometric profile stored in a chip in the document. The proposal ignored the clear limitation in Article 18(3) of the then EC Treaty stating that the power of the European Commission to adopt legislation to facilitate free movement shall not apply to provisions on passports, identity cards, residence permits or any other such document. With identity checks abolished in the Schengen area and those states outside determined to maintain them, the clause was devised to prevent the Commission overreaching on free movement or border controls. With the 2004 elections pending, the Parliament's Citizens' Rights and Freedoms Committee decided to leave its reports on the various EU biometrics proposals to the next parliament, explaining that:

> *The European Parliament is not in a position to endorse the proposals as long as the commission does not put its cards on the table and fully inform us of its strategy. We need proper democratic scrutiny of this far-reaching legislation, which in the worst case scenario could represent a step towards systematic registration of EU citizens' personal data* (Statewatch 2004a).

Following the elections, a new EP report supported the biometrics proposals in principle but rejected fingerprinting and any kind of EU population database/document register due to the data protection sensitivities and the risk of 'function creep' being 'too great' (European Parliament 2004). The EP also proposed a recital to the draft legislation stating that '…the European Council made a political decision to introduce biometric identifiers … without any input from practitioners and without knowing the magnitude of the problem, if indeed there is a problem' (ibid.).

In October 2004, while the EP Committee on Citizens' Rights and Freedoms was discussing this draft report, the Council changed its proposals again to make fingerprinting mandatory rather than optional. Rather than re-consult the Parliament – as is required following the significant amendment of a legislative proposal – the Council again invoked the 'urgency procedure', this time promising to introduce 'co-decision' on immigration and asylum policies if the EP complied with its demands, a process rightly described as 'blackmail' (Statewatch 2004b).

Despite an open letter signed by over 50 privacy organisations and data protection Commissioners across Europe urging MEPs to reject 'an unnecessary and rushed policy that will have hazardous effects on Europeans' right to privacy' (Privacy International et al. 2004), the EP report was adopted and the EU legislation was nodded through by JHA ministers in December 2004 with no further debate.

## 2.3. Database states

Counterterrorism combined with technological advance had provided the justification for mass fingerprinting across a continent that had for the best part of a century only fingerprinted criminals. With harmonised EU documents containing biometric data came a new generation of national and EU biometric databases.

The Visa Information System (VIS) has been operational since 11 October 2011. The central VIS database keeps data from all visa applications (including those applications that are refused) for a period of five years (European Commission 2015a). This includes all 10 fingerprints and a digital photograph from persons applying for a visa for the first time, for instance at a consulate of a Schengen state. The first consular posts to be connected to the system were those in Algeria, Egypt, Libya, Mauritania, Morocco, and Tunisia, followed by Israel, Jordan, Lebanon, and Syria. At the Schengen area's external borders, the visa holder's fingerprints are checked in order to verify the identity of the visa holder. Eventually, the central database is expected to include as many as 80 million visa applications. In addition to the Schengen states' authorities responsible for visa applications, asylum authorities – and in specific cases EUROPOL and national law enforcement agencies – may request access to VIS data for the purposes of preventing, detecting, and investigating terrorist and criminal offences.

Although there was little appetite for an EU wide database of EU citizens' fingerprints, the fingerprinting of EU passport holders meant the creation of national databases. However, as early as 2003, some member states had sought to make their databases interoperable, allowing police forces to search for the fingerprints of wanted persons (e.g. from crime scenes) across the databases of another on a hit/no hit basis. The proposal was formalised in the Prüm Convention, a treaty signed in 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain. Participation was later opened to other member states and more than half now participate (EU Council 2005).

The subsequent addition of biometrics to the profiles in the Schengen Information System (SIS) – the EU wide database of 'wanted persons' and stolen goods – meant that the search facility would effectively work both ways, with persons entering the Schengen area or apprehended by national police checked against 'wanted' profiles in the SIS/SIS II database.

## 2.4. Smart borders

The introduction of biometric travel documents also precipitated the introduction of so-called 'smart borders'. For the EU, this was initially premised not on national security but immigration control, with security viewed as a secondary but nevertheless important consideration. The European Commission's 2008 'smart borders' package highlighted the lack of pre-frontier controls on non-visa nationals: 'From a security angle, third-country nationals not requiring a visa are currently not subject to any systematic

check for border control purposes before arriving at the border itself' (European Commission 2008). Put another way: nationals of countries not subject to the EU visa requirements (those on the so-called 'white list') were not subject to either fingerprinting or the visa application process, and could simply travel to Europe and receive a Schengen visa upon arrival.

The Commission's 2008 'smart borders' package comprised:

- a 'Registered Traveller' Programme (RT) for 'low risk' travellers from third countries, including those that are subject to the visa requirement and those that are not, based on the pre-screening and collection of biometric data from applicants;
- the introduction of 'Automated Border Control' (ABC) gates to speed the entry of 'bona fide travellers' (EU citizens and pre-registered travellers);
- an 'entry/exit system' (EES) providing for the 'automatic registration of the time and place of entry and exit of third country nationals, both those that require a visa and those that do not, to identify overstayers';
- an Electronic System of Travel Authorisation (ESTA) to screen third-country nationals not subject to the visa requirement to verify that they fulfil the entry conditions before travelling to the EU.

It would be five years before formal proposals would be issued, and by this time the plan for an ESTA system had been dropped. The 2013 proposals would have created an Entry-Exit System, under which *all* third country nationals entering the Schengen area/EU would be fingerprinted and registered, with an 'alert' issued for those persons whose exit was not recorded by the EES within the time frame within which they were entitled. The costly proposals (put at over €1 billion), were thus justified primarily on immigration grounds, with the aim of combating visa 'overstayers'.

These were shelved for two reasons. Firstly, the member states saw little value in the EES if it did not have a law enforcement/security purpose; secondly, a report commissioned by the European Parliament cast significant doubt on the merits of the cost estimates in the Commission's feasibility study. In the meantime, more and more member states began rolling out their own 'smart borders' programmes.

In April 2016 the Commission issued revised proposals for EU smart borders, now comprised only of an Entry-Exit System employing Automated Border Control gates, with the decision to establish registered traveller programmes left to member states, subject to adherence to minimum EU standards (European Commission 2016b). Sparked by terrorism and a dramatic increase in the number of asylum seekers, including fears of terrorists posing as refugees, the proposals also had a revised justification: 'promot[ing] mobility between the Schengen zone and third countries in a secure environment', while providing 'an additional instrument to prevent and combat terrorism and serious crime, by tracking travel patterns and combatting document and identity fraud'.

There will also be enhanced interoperability across the various EU and Interpol databases, allowing '…simultaneous searches [facilitated by] a single search interface at national level… to ensure that all relevant information is available to border guards and/or police officers when and where this is

necessary for their respective tasks' (European Commission 2016d). This kind of 'interoperability' has the effect of creating a single database by centralising access to multiple sources rather than centralising the data. It also renders the firewalls that were meant to ensure that databases established for one purpose were only used for such purposes largely redundant (see Jeandesboz, Rijpa and Bigo 2016).

## 2.5. Summary

The regulation of biometric technologies of identity management and criminal forensics policing in the EU demonstrate how the introduction of technology for a limited purpose may generate incentives for new uses. Starting out with the registration of refugees, the EU has integrated biometrics as a technology of governance in spite of political controversy and advanced data protection regulations.

Mandatory biometric profiling coupled with the incremental expansion in the purposes for which the profiles may be used and the law enforcement and immigration control systems to which they are linked raises various concerns and objections. However, because the legislation has developed in piecemeal fashion under the auspices and complexity of the EU, these have been subject only to the minimum of debate by national parliaments or European citizens, the vast majority of whom will have no idea about the nature of these developments or their potential consequences. Regardless of whether individuals are accepting of these kinds of measures or not, in the absence of a public debate in which citizens are genuinely informed about the existence, purpose, scope and implications of policy-making by a critical media embedded in a wider political culture, such measures will continue to lack meaningful democratic legitimacy. As Ashbourne suggested a decade ago:

> *The current focus upon identity management and the globalisation of identity management is somewhat bizarre. It is out of all proportion to the claimed benefits and clearly politically inspired. This is somewhat distressing to see, particularly within European Union member states who, typically, one would like to think would adopt a more societally sympathetic stance. Proposals are consequently being rushed through without proper debate, without an understanding of the societal implications and without reference to an agreed longer term strategy... The problem is we have an 'emperors new clothes' syndrome, whereby there are few who are prepared to stand up and take an objective view of things, and even fewer who are prepared to listen. This situation must change if we are to avoid the more negative associations of identity management* (Ashbourne 2006).

Ten years later, the systems that employ biometric profiling are still in their infancy. Racism, xenophobia and right-wing populism is resurgent across Europe. As a new generation of hand-held fingerprint scanners is rolled out to police forces and illegal immigration 'hit squads', one might ask what will prevent the realisation of the most authoritarian and dystopian scenarios for biometric profiling and immigration enforcement.[21]

[21] On these developments in policing, see e.g.: http://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf, p.17; http://www.bbc.co.uk/news/technology-18188677; http://www.statewatch.org/news/2013/jan/12-eu-mobile-identification.html.

The answer presumably lies in legal regulation based on ethical considerations of the social and political, as well as personal, impact of the technologies. In the next sections, aspects of this societal dimension are further investigated. Widening the scope to global developments, they identify examples and issues of crucial importance when new applications of biometrics are considered in a European context.

# 3. Transforming social institutions

Massive digitization and the utilization of biometric technologies in individual IDs in recent times have allowed for different sectors and social agencies to become networked through identification systems. Databases are at the heart of this development, as databases open for the sharing of data across territorial boundaries, creating new forms of networks, for tracking and tracing individuals, and for the usage of algorithmic searches and profiling techniques. Large collections of information and data on individuals - Big Data – also bears massive potential for assessing trends and forming predictions on people's behavior and movement.

As we have seen, the usage of biometric technologies to form large scale and networked systems are increasingly becoming common, on both national and transnational levels. Consider for example the US-VISIT programme, which, when developed post 9/11, was the world's largest biometric database (now clearly surpassed by India with its 1 billion biometric database). The US-VISIT programme relied on dataveillance to categorize populations according to degrees of risk, a process that was achieved through interfacing of multiple different databases including those from health, financial and travel records, police authorities and more (Amoore 2006). Since then, countries have increasingly been seeking to integrate biometric identification practices under more centralized systems that rely on single large-scale databases that allow for usage across societal sectors as well as the concentrated accumulation of data and information on populations to be used for algorithmic calculation.

This section looks into recent large-scale biometric identification projects in order to investigate the different ways in which social institutions utilize biometric databases and identification practices, and how social institutions interact through this process. To what extent do biometric technologies facilitate interaction between different social institutions, and which kind of interaction do they (co)produce? What are the underpinning values and intentions when introducing larger cross-territorial or cross-sectoral biometric databases?

## 3.1. Biometric technologies and the interactions they produce

The collection and flow of data on populations and the interoperability of biometric data collections is increasingly becoming a global agenda. A national example of this development is Estonia, promoted as 'one of the most advanced e-societies in the world' (Estonia.eu 2016). Almost its entire service delivery of social institutions, including health, education and finance, is provided through digital IDs. Estonia has furthermore recently introduced e-citizenship, with the purpose of granting the rights and opportunities of citizenship to people who reside outside of the border of the 1,3 million populated country. By acquiring digital ID cards and digital signatures, people will get access to Estonia's numerous databases and services. E-passports are in this way expected to provide gateways for investments, business and act as a portal for collaboration in other European countries. It is expected that in the coming years, the country's population will increase 600%, from 1.3 million to 10 million through e-Estonia promotion (ibid).

With the model of Estonia as the most advanced application of national e-governance, other countries within and outside of the EU are increasingly seeking to create national identification portals for service delivery. In line with the positive narratives outlined in section 1, the political rationale of the wide

application of biometric technologies is primarily based on two interlinked factors. First of all, the technology enables seemingly accurate and precise oversight over peoples' movement through the interlinking of biometric data with large networks of databases. When integrated into national IDs, biometric tools enable an oversight of residents, the means to define insiders from outsiders, and making populations knowable. Secondly, biometric identification technologies in information systems enable rapid identity verification, facilitating efficient and real-time flow of digitalized information. Individuals' health records, welfare status, educational records can be virtually traced and shared, and assets transported through large-scale interconnected banking systems, thereby securing growth trajectories.

As already mentioned in section 1, the World Bank with its ID4D is at the forefront of promoting national identification systems which are built in such a way as to use biometric data of registrars across government services and social institutions. In a recent report, the steps to achieving a national biometric platform for such an all-encompassing biometric usage is outlined:

> *In pursuing sectoral initiatives relating to identification, countries tend to develop parallel systems, which oftentimes are neither connected nor interoperable. Therefore, nations seeking to roll out ID initiatives can benefit from adopting a standards-based approach and by linking national ID programs and sectoral interventions. This can result in enhanced interoperability of systems and use cases. (World Bank 2015: 2-3)*

According to the report, the larger the integration of biometric data usage, the more advanced is the country in its digital potentiality. The argument for such an interoperability and interaction in biometric registration and processing of biometric data is first and foremost that this will minimise costs, and that it will enable further prevention of fraud and duplicates:

> *Countries that have integrated their ID systems with their functional registries can more easily track benefits accessed by each user and can minimize benefits leakage (in forms such as 'ghost' payroll payments or duplicated subsidy payments). (World Bank 2015: 7)*

Tracking and tracing of both individual behaviour and movement, but also that of flows of money and goods, here become a core achievement that countries should strive for. The higher the potential of sharing data on individuals across services, the better potential for eliminating fraud and minimising costs. This cost-effective calculation also includes taking stock of legal protections of individual rights, such as privacy and data protection, but also finding ways of manoeuvring within existing legal landscapes. Values such as efficiency, elimination of fraud and the minimization of costs and leakages, are also essential to other forms of interoperative biometric schemes.

The promise of a truthful identification and the possibility to track and trace movement support the widespread implementation of biometric schemes. This logic also prevails in the European sharing of biometric data (EURODAC), India's national biometric project and the usage of facial recognition technology in UK's policing, as will be discussed below. These cases are highlighted as they are large scale examples of how the use of networked, searchable databases have become central to today's biometric ID systems (c.f. Lyon 2009). Biometric ID systems provide unlimited conditions of possibility:

> *What is significant about the big data moment is not simply that it has become possible to store quantities of data that are impossible for any individual to comprehend (The Library of Alexandria did that, as does the night sky, and the human brain), but the fact that this data can be put to use in novel ways—for assessing disease distributions, tracking business trends, mapping crime patterns, analysing web traffic, and predicting everything from the weather to the behavior of the financial markets, to name but a few examples.* (Andrejevic and Gates. 2014: 186)

What is apparent in the discourses that support the networking of biometric databases is the notion and assumption that the more biometric data that is collected, the more basis there is for governance and policing. Large biometric databases and systems allow for the sharing and accumulation of data across different social institutions, and for interaction and sharing data across sectorial divides. Because of their inherent mathematical nature, biometric data collection in database systems also bring about the promise of possibilities of aggregating data, the creation of statistical normalities on an overall sample group, the formation and utilisation of lists and the creation of individual profiles.

## 3.2. Case studies

### *3.3.1. Counter terrorism and policing: facial recognition in the UK*

The usage of biometrics in policing and counter terrorism measurements has increased the last decade. Indeed, the rise of biometric identification technologies and other forms of surveillance techniques, are underscored by the '[…] use of risk as a means of governing in the war on terror, based on dividing practices that segregate 'legitimate' mobilities (business, travel, leisure and so on) from 'illegitimate' mobilities (terrorist, trafficker, immigrant and so on).' (Andrejevic and Gates. 2014: 186). A principle understanding of such technologies is that increased surveillance and data collection will lead to more secure and precise forms of sorting.

The video image of the two alleged 9/11 attackers Mohammad Atta and Abdulaziz Alomari passing through security at the airport in Portlain, Maine, has become part of the 9/11 iconography (Gates 2011). Since then, the world has been provided with video evidence of both of the Boston Marathon bombers, and the bombers of Brussels airport. Undoubtedly, the usage of images of faces captured by surveillance cameras as a unique identifier has become a common technique of policing across Europe. Among the states in the region, the UK is by far the country utilizing video surveillance the most. The UK is the world's most surveilled country through CCTVs. In recent years, police and counter-terrorism agencies have increasingly sought to use such 'videoveillance' as a means to combat crime and for counter terrorism purposes.

The accumulation of data in biometric databases and their networked systems, can lead to practices that are not thought of in the initial phase of their development. Furthermore, persons who have no history of criminal offences, or any other action that should lead to their biometrics being included in such networks, might find themselves part of databases without their awareness. More than half of the individuals recorded in the UK's national counter-terrorism biometric database, for example, have never committed any criminal offence (MacGregor 2016).

This is particularly potential in cases of automated recognition that becomes possible through the algorithmic nature of biometric technologies applied in digital networks. This can lead to various forms of data mining and individual profiling – for varying purposes including commercial gain and policing – and close monitoring of individual behavior. Noteworthy here, Facebook has removed facial recognition from its sites in Europe because of the power of facial recognition technologies also for commercial profiling and data mining and the legal concerns it has created in several European countries (c.f. Hern 2016).

The face of a person is her most common means of communicating with others, and a foundation for social interaction. It is uncommon to hide one's face, and the practice of hiding the face is in European societies seen as a reason for suspicion. Furthermore, '[…] face images are routinely collected in society by a variety of institutions, such as when we apply for a driving license, or a passport, or a library card, etc.' (Itrona and Wood 2004: 178).

Because of the fact that they are used in multiple social institutional and public environments, the utilization of facial recognition technologies for policing and counter terrorism efforts bear the potential of a 'perpetual lineup' (Garvie et al. 2016), whereby the law enforcing agencies have the possibility to check facial images of people in different settings- through CCTV of public spaces, driver license databases, social media and networks such as Facebook, etc. without their knowledge.

In recent years, the UK police have begun using their databases for face recognition scanning against public crowds. One example of this was when the Leicestershire Police in 2015 utilized facial recognition technology to scan the 90.000 people who were audience of the Derby's Download rock festival. Facial images of the festival audience were cross-compared with a criminal database. This practice was again tested in 2016, when London police utilized facial recognition technology at the Notting Hill Carnival, which involved the '[…] use of overt cameras which scan the faces of those passing by and flag up potential matches against a database of custody images.' (Metropolitan Police 2016). Having studied the utilization of such technologies in the US, Garvie et al. (2016) summarize this problematic:

> *A face recognition search conducted in the field to verify the identity of someone who has been legally stopped or arrested is different, in principle and effect, than an investigatory search of an ATM photo against a driver's license database, or continuous, real-time scans of people walking by a surveillance camera. The former is targeted and public. The latter are generalized and invisible.*

Facial recognition technologies and combined with the new scales of large networked digital systems bring about new potentialities for commercial profiling and policing. They allow different social institutions – including police, social media and different agencies such as trafficking – to interact and share information. However, as we can see in the above study, this interaction is not unproblematic. It brings about new forms of societal interaction and surveillance that has to be taken into consideration in legal and ethical debates on its increased usage.

### *3.3.2. Asylum and refugee registration in Europe: EURODAC*

In the latest years EU members have gathered the management of people who seek protection (asylum, refugees) under the framework of the Dublin Regulation. In order to facilitate the application of this regulation, the EU has introduced EURODAC, a biometric database in which Member States are obliged to enter the biometric (fingerprint) data of irregular migrants or asylum seekers (see also discussion in Section 2). The purpose is to identify where they entered the EU, whether if they have previously made protection claims, and furthermore assign responsibility for the asylum claim to the member state where they first made their entry. In its original function and purpose, the EURODAC database was strictly limited to the application to matters regarding asylum. However, now newer regulations allow national police forces and Europol to '[…] compare fingerprints linked to criminal investigations with those contained in EURODAC [...] for the purpose of the prevention, detection and investigation of serious crimes and terrorism.' (European Commission 2016c)

The interoperability and sharing of biometric data of asylum seekers with law enforcement agencies is beyond the original mandate of EURODAC and has raised several concerns regarding its potential social and political consequences. The UNHCR, as an organization with the mandate to protect refugees, has expressed that:

> *[…] this change may lead not only to interference with the right to privacy and family life of asylum-seekers and refugees, but it may also place a refugee and his/her family at significant risk of harm, if the information is shared with countries of origin. It may also result in stigmatisation of asylum- seekers as a group by associating them with criminal activity. Furthermore, UNHCR takes note that the proposal to include the possibility to search latent fingerprints relies on technology in which the risk of error has not been fully examined and eliminated (latent fingerprints).* (UNHCR 2012)

Biometric registration is on the one hand a technocratic practice, but on the other hand it is also an experience and a practice that has social, ethical, legal and political consequences. Fingerprinting of persons seeking protection as a border management tool is driven by the twofold principles of guaranteeing rights and secondly controlling movement. The consequence of blurred intentions and practices with biometric registration may have unfortunate consequences.

Identification practices and the establishment of ID vis-à-vis the host country on the one hand grants a formalized identity and 'rights' as refugee, but it also limits their opportunities and possibility of disappearance. The rationale and practice of digital biometric registration alters governance and the relationship between governing authorities and the subject, as it places the biopolitical question 'who are you?' as a foundation for such relationships (c.f. Pugliese 2010). At the same time, once captured in a biometric database, the refugee's movement is tracked and traced. There is thus a tension between the need to be identified in order to achieve/claim rights - once that registration takes place, one becomes part of a system that also seeks to surveil and control one's movement.

Indeed, the issue of fingerprinting and the consequences of this practice on the life of those seeking asylum has been an issue of contention, especially in the latest year. Since the refugee crisis in 2015, EU member states have entered a series of discussions regarding the process of biometric registration of persons who seek protection. Fingerprinting of persons entering EU member states from 3rd

countries through informal routes is not only compulsory, but also debated. Refugees from Syria have been found to erase fingerprints and to object to fingerprinting. Because of the fact that some of those seeking protection object to fingerprinting, discussions on compulsion and consent are also central to these practices. This has caused a debate in the European member states about the issue of coercion, and if coercion can take place, the extent of coercion that can take place in identification practices (European Commission 2015b).

### *3.3.3. India's biometric scheme: national IDs for multiple purpose*

In India, the entire population of about 1,2 billion people are being biometrically registered. The nation-wide Unique Identification Scheme (UID) in India was initiated in 2009, and rapidly grew to become the largest biometric scheme in the world. The biometric data is then stored in a centralised database, which to date has the biometric data of 1 billion residents. The main stated objective of the scheme is to provide identification to all Indian residents, and hence be a foundation for inclusion of poor and marginalized through giving them access to private and public services (UDAI 2010). Unique IDs are to serve as a foundation –*Aadhaar*– for the distribution of benefits. In India, the introduction of biometric ID is, on the one hand, a national strategy, and on the other, a multilateral development and inclusion strategy, in which India is taking the lead in a rapidly growing software industry. It will furthermore serve to network national security agencies and advance tracking of individual identities. The Indian Unique ID project is thus a congregation of discourses and practices of various fields, including security, commerce and welfare (Jacobsen 2012, 2015).

The UID scheme in operation serves as a pilot project for similar developments in other countries, as one of the first of its kind to place IDs at the heart of an ambitious development agenda (Jacobsen 2015). The World Bank's report on ID4D (2015) significantly draws on India's project, which serves as the template for other national biometric identification schemes. The development of the scheme is of interest to Europe as well as globally, as it is presented as a template for other countries who are seeking to utilise biometric IDs as a foundation for governmental and security purposes, showing how interoperability can be optimised across different governance fields (i.e. security, welfare, commerce). This case and the development of biometric in a country as large as India, are relevant to a study of biometric practices in Europe, as it shows the multiple ways in which countries are using the technology, and furthermore is part as a larger global trend in which emerging economies and countries in the so-called global South are utilising nationalised biometric identification schemes for multiple governmental domains, including those of security and border control, welfare delivery and cash transfers, health and education (see the integration of government functions described in Section 1).

The centralized nature of the UID project, as well as the possibilities it opens up for minute tracking and surveillance, has raised questions among Indian commentators (Dass 2011, Mehmood 2008, Ramanathan 2010, Shukla 2010). The debates have centred on whether the Unique Identification number will eventually be obligatory because of its widespread application in required government schemes, the possible violations that the biometric scheme may pose on privacy and civil liberties, and the extent to which the scheme will tap into intelligence and police databases through function creep. Questions have also been raised regarding the possible distortions built into the technology itself,

which will lead to a massive exclusion of 'unreadable' bodies should the ID number become mandatory for accessing services.

The abstracted notion of inclusion built into the scheme risks excluding the very people it is claiming to include. Persons who are all day on the streets doing hard manual labor, or who have certain kinds of diseases, will have trouble being recognized by the biometric system, because for instance their fingerprints might not be readable or their irises not recognizable. Scholars are therefore wary that the increasingly widespread usage of biometric ID may create new forms and mechanisms of social exclusion (Magnet 2011, Monahan 2009, Aas 2006), especially through obscuring social inequalities and gender differences.

### 3.3. Summary

At the heart of the widespread usage of biometric technologies and their expanding employment in large, international systems of data sharing, are two main claims, 1) people need identification in order to claim rights, 2) people need to be identified truthfully to prevent fraud/impersonation/terrorism. In the abovementioned examples of interoperability in biometric registration, the main common problem that biometric identification is to solve is matters regarding trust. Fraud is to be eliminated in the Indian state service delivery system, the asylum seeker or migrant entering European soil is to be identified in order for her identity to be truthfully verified at a later entry point within the regional map, the potential criminal or terrorist is to be prevented from faking identity. However, networking of data across social institutions also adds several new conditions of possibility beyond merely a practice of identification and verification.

The widespread usage of biometrics in networked systems that bind social institutions in as differing fields such as security, welfare, banking and policing, lead to the potential of tracking individuals and governing mobility and behavior. As such, they allow for the possibility of aligning new forms of societal borders, defining insiders from outsiders, and 'designating the safe from the dangerous at multiple borders of daily life' (Amoore 2006). The final section will consider the socio-political implications of biometric technologies in some more detail.

# 4. Impact on non-technical bonds of community

Biometric identification has effects on the individual body and personal identity (section 1) and entails new possibilities of social control and social exclusion, as the preceding section has shown. Yet potentially more radical even, biometric recognition may have implications for the very nature of the modern socio-political institutions of the subject, society and the state. This entails the changing nature of social communication, processes of user fragmentation and desocialisation and the decentralization of authority that shall be addressed briefly in turn in closing.

Indicating relevant perspectives and theories, the objective of this section is to identify political transformations that may be at stake when biometrics are integrated in advanced data based governance. The full treatment of this subject is beyond the scope of this report and involves the evaluation of future scenarios.

## 4.1. Coded communication

As Aas (2006: 151) has argued, biometric identification produces a transformation of the nature of communication that has 'profound consequences for the nature of sociality and social norms'. This transformation is rooted in a shift from biographical narrative to identity as coded body conveyed through symbols devoid of meaning (2006: 155). In eliminating the possibility of doubt, error and negotiation and erecting a 'binary universe of acceptance or denial, positive or negative, right or false' (2006: 151) the space for action and the limits of social interaction are set in advance. Instead of the negotiation of trustworthiness through narratives, discourse and argumentation, the 'whole existence of the user is condensed into specific legitimizing signals which are the only meaningful elements of the system' (Lianos and Douglas 2000: 106). Technological systems do not make decisions on the basis of 'whole persons' with a coherent, situated self and a biography, but on the basis of 'singular signs' (Aas 2006: 155). If character evaluation, danger and trustworthiness are converted into simple empirical questions of false and positive that can be answered by technology, the 'need for shared cultural and normative contexts or any common understanding of the actors involved' (2006: 152) evaporates. The elimination of fraud also eliminates the significance of the quality of trust, or at the very least, 'accelerates the trend away from persons towards data images as the basis for trust in society' (Wood and Graham 2014: 182, Lyon 2001).

## 4.2. Open bodies

The changing nature of communication has significant effects on the nature and quality of the bonds of community. In the occidental tradition of state theory it has been the image of the social body that founds and communicates society as unity and entity, marks the inside and outside of the political body and provides a means of identification that signifies more than the sum of its parts (Frank *et al*, 2002: 78). Social cohesion has been seen to be forged by the logic of the image of the body metaphor, including specific expressions of the nature of the bodily image, the relation between individual body and collective body, and the representative form that embodiment takes (Koschorke *et al* 2007). With the externalisation of intrinsic features operated by biometric ID, 'what were more or less closed systems, my body, the social body, becomes more or less open constellations. My body cannot

interface with technological systems unless it is more or less open' (Lash, 2002: 16 in Aas 2006: 152). The opening of the individual body goes along with the opening of the social, or collective, body. The collective border has become the portable border and the 'body as carrier of the border inscribed with multiple encoded boundaries of access' (Amoore 2006: 348). In this relocation of the border, the nation state's 'implicit definition of the 'other' is built into automated systems for determining who is a member' (Lyon 2005: 79) - 'the border is everywhere'. Because of the instantaneous communication of information, biometric ID also alters the geography of centre and periphery (2006: 152) into more equivalent chains of communication, enabling a government at a distance (Rose 1996, Garland, 1997) that simultaneously increases the local impact of decisions.

### 4.3. End of the social?

As section 3 noted, the opening of the body provides new parameters for social control and possibilities for social discrimination along various lines. The 'problem with automated systems is that they aim to facilitate exclusionary rather than inclusionary goals' (Norris *et al* 1998). Biometric ID is part of a broader spectrum of using biological data as means of social identification and risk management. But in addition to opening individual and collective bodies, biometrics has also been argued to effect a decline of collective sociality and the broad visions that underline political bodies and control as such. This tendency can be observed in many different contexts of biometric applications: The global war on terror has been said to entail 'a more pronounced donor focus on *individual* refugee data (as different from *aggregate population* figures)' (Lindskov Jacobsen 2016: 159). There is a growing interest in remote technologies and retreat from the uncertainty of face-to-face encounters within disaster zones (Duffield 2015: 85). As Lianos has noted, biotechnology effects a new model of control that is

> *'neither intersubjective nor group-based. On the contrary, it is by definition impersonal in its origin and atomized in its reception […] The growing emergence of precision in the delivery of services […] makes the capitalist market and the Western State unable to function without users who are completely individualized in their contacts with administrations and businesses. A remote, often invisible and diffuse, entity provides its services to isolated individuals' (2003: 416).*

This new type of control is profoundly atomizing because 'it is indispensable for the controlling device to deal with identifiable – thus indictable – individuals' (ibid: 424) and avoid collective effects capable of distortion. This means that in place of the 'broad, moral and disciplinary, modernist vision of control' sociality is 'increasingly governed by inhuman rules of automated flows which are orchestrated and enacted through enormous systems of interlinked and computerized elements using code'. According to Lianos (ibid: 423-25), biometrically encoded control entails both a process of desocialisation – that is, the rapid disengagement of users from social belonging – and a process of de-subjectification of the individual, which 'is being largely transformed into a fragmented user'(2003: 423).

This argument relies on a literal translation of the technology of biometrics into social effects. Presumably, it underplays how the technology will always be embedded in social practices that cannot be reduced to the rationale and features of the technology as such. For instance, refugees entering Europe strategically adapt to the identity management system, for instance by avoiding

entering the EU through Cyprus where access to the Schengen area is restricted. Also the states do not follow the technology blindly. Instead, they combine the systems of refugee registration with pragmatic concerns of burden sharing and justice. Yet, the reliance of biometric systems of identity management on data on individual bodies rather than on the social identities and aspirations of those individuals may affect the role of the social as a political category. Indeed, this is a consideration that is worth investigating further through concrete cases like the ones introduced in the previous section.

### 4.4. End of the state?

Biometric identification has been associated above with an expanding apparatus of surveillance and the interoperability of national databases often imagined in terms of 'Big brother' scenarios of totalitarian state empowerment. Yet as some scholars have argued, biometric identification may also entail a promise to 'liberate citizens from the 'tyranny' of nation states and create a new global decentralized, rhyzomatic scheme for personal recognition' (Mordini and Massari 2008: 496). As they see it, modern states have since their emergence 'expropriated from individuals and private entities the legitimate means of movement' (ibid). One of the main sources of power of states thus resided in the registration of birth certificates and the administration of citizenship. Biometric systems are seen to have the potential to retrieve the power of identification from states because they are 'the only large-scale identification systems that could also be run by small private actors and independent agencies instead of heavy governmental structures' (ibid). With a system of identification that in its structure resembles the Internet more than the Leviathan, biometrics could provide a 'sound identity system for global citizens that could develop quite independently of nation-states' (ibid). The rationale behind this motion is also reflected in the motivation behind the creation of digital currencies, such as Bitcoin. The blockchain technology that originated with Bitcoin in 2009 and is envisioned to be extended beyond finance to areas such as government, health and science operates on principles profoundly adverse to the political organization of modern states. A blockchain is a permanent public database or ledger that is distributed among all the nodes in the network, where each node has a complete copy of the total database (DuPont and Maurer 2015). Transactions taking place are competitively verified and guaranteed by individual nodes based on their computational power (and rewarded by Bitcoins), thus eliminating the need for a trusted third party. This includes the need for clearing houses and settlement parties, but also for the role of state authority in underwriting currency and enforcing contracts, or the role of banks in monitoring and assuming risk and generally mediating payments. In placing the security of transactions in transparent public proof and in the economically incentivized self-policing of the system, blockchain in effect appears to dispense with the need for centralized authority. The nexus of biometric identification and digital networks also has radical implications for conceptions of the public. The digital public has been said to be less a 'sphere' than a sequence of referential linkages with no (imaginary) boundaries (Langenohl and Wetzel 2013). In this vision of the digital age, the public is no longer normative, or the result of processes of social differentiation, but equals the production of particular networked publics for specific acts of communication (2013: 11).

### 4.5. Summary

Beyond the transformations of human nature and personal identity and beyond new forms of social control and discrimination that have been analysed in the previous sections, biometric technologies are a central part of a paradigm of control that may be set to alter the very socio-political foundations of modernity. Biometric systems alter the fabric of communication from narratives, negotiation and norms to codes and technical rules of action with predefined limits of social interaction. According to the four perspectives outlined in this section, this implies that current systems of the subject/citizen and the social body are replace by open fragmented bodies, entailing a demise of collectivity, social belonging and the identity generating function of social metaphors. The centralized and integrated visions of control increasingly give way to systems that favour the 'fluid – albeit atomized – channeling of individuals' (Lianos 2003: 425). Biometric systems have been seen as identification systems that for the first time in history could operate quite independently of states, emulating the motivation of the blockchain technology as radically decentralised and self-policing networks. Yet, to what extent states will be affected by this, or not in fact be capable of instrumentalising even 'anti-statist' technology, remains to be seen.

## Conclusion

The combination of new biometric technologies with advanced cloud based computing and big data analysis in governance programs, policing and commercial services hold the promise of advancing the security and welfare of societies. Compared to established biometric systems based on finger prints, face recognition and DNA, this changes the ethics of biometrics.

Previously, ethical concerns have been raised regarding the impact of biometrics on the life of individuals, including issues of privacy, discrimination and the protection of sensitive personal data. These worries have been related to problems of function creep, the reliability and accountability of biometric data, the reduction of human identity to biological information, and the emergence of new forms of economy and surveillance. Yet, the implications of these problems are not fully grasped through a focus on their impact at an individual level. They require a complementary focus on their effects on social relations and political order. This is the focus of the societal ethics of biometric technologies.

In the European Union, the collection and processing of biometric data has been effectively regulated through data protection regulations, shielding the privacy of European citizens. Limited to the registration of refugees and criminals in restricted databases and procedures, the collection and sharing of biometric data of entire societies has been considered an obvious breach of Article 8 of the Charter of Fundamental Rights of the European Union (2012) concerning the right of individuals to the protection of personal data. According to this article 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

It is hard to imagine how schemes for the processing of biometric data of all travellers crossing the borders of the Union, or the introduction of a system of 'smart borders' based on biometric identification, can be harmonized with this regulation. The same can be said about second generation technologies for the automated recognition of face, voice or behaviour through cameras and internet surveillance – techniques the require the building of massive registries of biometric data. Yet, these are among the current developments that are considered by EU policy makers.

Cases can be made for the legality of these measures, with reference to their expediency for protecting European societies from terrorism and serious organized crime. Furthermore, advanced techniques of privacy and data protection 'by design' – building relevant legal provisions into the systems – are being introduced. In effect, the systems come across as legal and 'ethical' without resolving the broader societal dimensions that exceed an individual centric focus on the ethics of biometrics. Legal arguments can therefore not resolve the issue alone. Ethical considerations of the values and principles underpinning the law are needed, both for the application and the adjustment of current regulations. Ultimately, the introduction of new technologies of security is a political question, demanding informed political debate.

In this connection, relevant cases from around the world are instructive. In section 3, three such cases were introduced: counter terrorism and policing through facial recognition in the UK; the EURODAC system for asylum and refugee registration in Europe; and India's massive biometric scheme of

national IDs for multiple purpose. Without exhausting their ethical or political implications, these case studies suggested several societal dimensions that require critical consideration.

In section 4, four perspectives for such consideration were outlined, referring relevant theories and literatures: coded communication; open bodies; end of the social; and end of the state. In addition to the analysis of current practices and historical examples, an essential aspect of these perspectives is the future social and political consequences of current political decisions. It is only by thinking through such scenarios that the societal ethics of pivotal political dilemmas can be properly addressed.

Combining the four perspectives, elements for further consideration include:

**Effects on the social bonds of community – of trust, belonging and of mutual care**. As argued by Ashbourne (2006), the causes of problems like crime, terrorism or deprivation are not a lack of effective identify management and surveillance but social issues that require a different kind of policies than policing and control. The introduction of biometric systems of security management may create a false sense of security while reducing the sense of collective responsibility.

**The division of power between citizens and the state**. While seemingly empowering law abiding citizens in the face of crime and violence, centralised biometric databases of the kinds of India, Kuwait and Estonia represent a powerful tool for the control of populations. When used in perfectly democratic countries, this control is supposed to harmonise with the will of the people. However, even in Europe no democracy is perfect, and the technologies themselves alter the relationship between the state and the citizen. Furthermore, the political systems may change, for instance as a result of war or occupation. Just think of the role of registries of personal data in the prosecution of Jews during World War II. When used in countries with a high level of political conflict, the integration of advanced biometrics in government programs may have a decisive impact on the outcome.

**Incentives of governments for respecting democratic rules**. Relating to the former point, effective measures of surveillance and policing may create incentives for governments to suppress political opposition and maintaining control of the state apparatus. If it is expected that the opposition will eventually use the same systems for the sake of repression and persecution, these anti-democratic incentives are reinforced.

**Impact on the objectives and procedures of government**. When political authorities can gather data on the identity of populations through the collection of biological material, it may reinforce a tendency to govern on the basis of advanced statistical information rather than through the consultation of the people. In effect, the citizens may lose their incentives and capacity for political participation, and the authorities may develop a false sense of representing the people through the processing of seemingly objective data. In a worst-case scenario, biometric data generate new ways of distinguishing between legitimate and illegitimate citizens, entailing racist programs of persecution on a seemingly scientific biological basis.

**Relations between citizens: inclusion/exclusion and mobility**. Biometrics is a major force in a paradigm of the automatic sorting of mobilities (Wood and Graham 2014: 183) through 'differential mobility' (2014: 177). This involves a risk of dividing contemporary societies into 'high-speed, high-mobility and connected and low-speed, low-mobility and disconnected classes' (ibid: 178) where

access and 'blockage' are becoming 'functions of encoded categorization' through biometrics (ibid: 179). Societies may then be divided between those who are enrolled in various systems of identity management and those who are excluded.

**The division of power between citizens, the state and private corporations**. Private corporations providing governments and citizens with biometric technologies build considerable capital in the form of biometric data on which the systems rely. In addition to controlling the data, the very capacity to manage the systems put corporate actors in a powerful position. This is also a lucrative position from which new commercial uses of the data can be developed, often by exploiting uncharted legal territory.

**Relations between states**. The sharing or stealing of biometric data from national schemes may alter the interaction and distribution of power between states (see e.g. Zwitter 2015). Cybercrime and 'cyber war' are considered as serious threats across the world, and with the circulation of personal data of the most sensitive kind upon which government programs and security systems rely, the stakes are raised further. Moreover, states are building databases of foreign nationals in the name of national security. The more effective the uses of these data are, the more valuable they are to intelligence services as well as for the commercial interests of states.

Principles of data protection and privacy are still relevant as a regulative framework for addressing societal issues like the ones listed above. Yet, they must be complemented by broader considerations of human rights and democracy, as well as principles like the non-intervention and self-determination of states. The decision on which norms to consider in a specific context does not follow from the above exposition of relevant ethical issues to address. Instead, this report has provided a starting point for making such normative decisions in particular contexts.

When applying the societal ethics of biometrics to concrete cases, it is necessary to distinguish between different kinds of uses of biometric technologies, as well as between different social and political contexts. Border management, criminal forensics, counterterrorism and welfare provision are dramatically different phenomena, requiring different ethical responses. Likewise, the collection, sharing, processing and application of biometric data imply separate ethical considerations. Hence, no blueprint solutions or general principles follow from the observations of this report. Instead, we hope we have inspired the reader to consider the societal dimension of specific cases, as well as critically evaluating current ethical, legal and political arguments on the legitimacy of biometric technologies.

## References

Aas, Katja Franko (2006) 'The body does not lie': Identity, risk and trust in technoculture, *Crime Media Culture* 2(2): 143-58.

Abergel, Elizabeth and Jamie Magnusson (2014) The Art of (Bio)Surveillance: Bioart and the Financialization of Life Systems, *Topia - Canadian Journal of Cultural Studies*, 30-31: 237-254.

Agamben, Giorgio (1998) *Homo Sacer: Sovereign Power and Bare Life*. Stanford: Stanford University Press.

Alterman, Anton (2003) 'A piece of yourself': Ethical Issues in Biometric Identification, *Ethics and Information Technology* 5: 139-150.

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

Andrejevic, Mark and Kelly Gates. 2014. Editorial. Big Data Surveillance: Introduction. *Surveillance & Society* 12(2): 185-196.

Ashbourne, Julian (2006) *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*. Background paper for the Euroscience Open Forum 2006, Munich. [online] Available at: http://www.statewatch.org/news/2006/jul/biometrics-and-identity-management.pdf (Accessed 30 November 2016)

Boy, Nina (2015) Report on the Theory of Risk as a Societal Security Instrument (SOURCE D5.1). Available at http://societalsecurity.net/source-deliverables.

Boy, Nina *et al* (2015) Analytic Report on the Impact of the Global Financial Crisis on Societal Security in Europe (SOURCE D5.3). Available at http://societalsecurity.net/source-deliverables.

Cooper, Melinda (2006) Pre-empting Emergence: The Biological Turn in the War on Terror, Th*eory, Culture and Society* 23(4): 113–135.

Cooper, Melinda (2008) *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle, WA: University of Washington Press.

Dass, Rajanish (2011) *Unique Identity Project in India: A Divine Dream or a Miscalculated Heroism?* Ahmedabad: Indian Institute of Management.

Duffield, Mark (2015) 'The Digital Development-Security Nexus: Linking Cyber-Humanitarianism and Drone Warfare' in Paul Jackson (ed) *Handbook of International Security and Development*, Cheltenham: Edward Elgar Publishing.

DuPont, Quentin and Maurer, Bill (2015) Ledgers and Law in the Blockchain. King's Review. 23 June. Available at http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/ (accessed 1 December 2016).

Estonia.eu (2016) 'E-Estonia'. Available at http://estonia.eu/about-estonia/economy-a-it/e-estonia.html (accessed 1 December 2016).

EU Council (1998). *Strategy Paper on Immigration and Asylum*. Doc. 9809/98, 1 July.

EU Council (2001) *German delegation proposal for a Council statement*. Doc. SN 4038/01, 27 September,

EU Council (2005) *Prüm Convention*, doc. 10900/05, 7 July.

EU Data Protection Directive (1995) 95/46/EC of the European Parliament and of the Council of 24 October 1995. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (Accessed 30 November 2016).

European Commission (2004) *Commission Staff Working Paper: Annual report on the development of a common policy on illegal immigration, smuggling and trafficking of human beings, external borders, and the return of illegal residents*. SEC(2004) 1349. Brussels 25 October. Available at: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2004/1349/COM_SEC(2004)1349_EN.pdf

European Commission (2016d – unreferenced) *High Level Expert Group on Information Systems and Interoperability – Scoping Paper*. Available at: http://statewatch.org/news/2016/sep/eu-com-hleg-interoperability-info-systems-scoping-paper-6-16.pdf (Accessed 30 November 2016)

European Commission (2008) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union*. Doc. COM(2008) 69 final, 13 February

European Commission (2015a) *Visa Information System (VIS)*. [online] Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm (Accessed 30 November 2016)

European Commission (2015b) *Commission Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints*. Available at http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/asylum/general/docs/guidelines_on_the_implementation_of_eu_rules_on_the_obligation_to_take_fingerprints_en.pdf (accessed 23 November 2016)

European Commission (2016a) *Proposal for a Regulation of the European Parliament and of the Council 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 examining 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*. COM (2016) 272 final, 4 May

European Commission (2016b) *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and*

*determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*. Doc. COM(2016) 194 final, 6 April

European Commission (2016c) *Identification of Applicants. EURODAC*. Available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm (accessed 25 November 2016)

European Parliament (2004) *Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports*. Doc. A6-0028/2004, 28 October

Frank, Thomas et al. (Hrsg.) *Des Kaisers neue Kleider.* Fischer Taschenbuch Verlag, Frankfurt am Main

French National Consultative Ethics Committee for Health and Life Sciences (2007) Biometrics, Identifying Data and Human Rights. *OPINION N° 98.* Available at: http://www.ccne-ethique.fr/docs/en/avis098.pdf.

Garvie, Clare, Alvaro Bedoya and Jonathan Frankle (2016) *The Perpetual Line Up. Unregulated Police Face Recognition in America*. Georgetown Law Center on Privacy & Technology. Available at https://www.perpetuallineup.org (accessed 1 December 2016).

Gates, Kelly (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York/London: New York University Press.

Hern, Alex (2016) Facebook launches facial recognition app in Europe (without facial recognition), *The Guardian*, Available at https://www.theguardian.com/technology/2016/may/11/facebook-moments-facial-recognition-app-europe (accessed 1 December 2016).

Hosein, Gus and Carly Nyst (2013) An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries. *Privacy International.* Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229 (Accessed 30 November 2016).

ICAO (2003) *Machine Readable Travel Documents - Specifications for Electronically Enabled MRtds with Biometric Identification Capability*. Doc. 9303P3-2, 28 May.

Introna, Lucas D. and David Wood (2004) Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2(2/3): 177-198.

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

Jacobsen, Elida K. U. (2015) *Unique Biometric IDs. Governmentality and Appropriation in a Digital India*. Gothenburg, University of Gothenburg: School of Global Studies.

Jain, A., R. Bolle and R.S. Pankanti (1999) Introduction to Biometrics, in (eds) *Biometrics: Personal Identification in Networked Society*, Kluwer Press: Dordrecht.

Jeandesboz, Julien, Jorrit Rijpma and Didier Bigo (2016) *Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal*. Study for the LIBE Committee, European Parliament.

Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU(2016)571381_EN.pdf.

Jlevy (2013) 'REACH: Linking Biometrics and Mapping in South Sudan.' Available at http://www.comminit.com/global/content/reach-linking-biometrics-and-mapping-south-sudan (updated 18 January). Accessed December 10, 2013.

Koschorke, Albrecht; Lüdemann, Susanne; Frank, Thomas und Ethel Matala de Mazza (2007) *Der fiktive Staat – Konstruktionen des politischen Körpers in der Geschichte Europas.* Fischer Taschenbuch Verlag: Frankfurt am Main.

Langenohl, Andreas and Dieter Wetzel (2013) Finanzmarktpublika: Moralitaet, Krisen und Teilhabe in der oekonomischen Moderne [Financial market publics: morality, crisis and participation in economic modernity]. Heidelberg: Springer VS.

Lebovic, Nitzan (2015) Biometrics or the Power of the Radical Centre, *Critical Inquiry*, 41(4): 841-868.

Lianos, Michalis (2003) Social Control after Foucault, *Surveillance and Society* 1(3): 412-430.

Lindskov Jacobsen, Katja (2015) Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees, *Security Dialogue*, 46(2): 144-164.

Lindskov Jacobsen, Katja (2016) UNHCR, accountability and refugee biometrics, in Kristin Bergora Sandvik and in Katja Lindskov Jacobsen (eds) *UNHCR and the struggle for accountability: Technology, law and results-based management*. Abingdon: Routledge.

Lyon, David (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham and Philadelphia: Open University Press.

Lyon, David (2005) The Border Is Everywhere: ID Cards, Surveillance, and the Other, in E. Zureik and M. Salter (eds) *Global Surveillance and Policing: Borders, Security, Identity*. Cullompton: Willan.

Lyon, David (2009) *Identifying Citizens: ID Cards as Surveillance*. London: Polity Press.

MacGregor, Alastair R. (2016) Further Report by the biometrics commissioner on issues raised in his 2015 annual report, Commissioner for the Retention and Use of Biometric Material, available at: https://regmedia.co.uk/2016/05/26/police_biometrics.pdf

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

Mehmood, Taha (2008) India's new ID card. Fuzzy logics, double meanings and ethnic ambiguities, in Colin J. Benett and David Lyon (eds) *Playing the Identity Card. Surveillance, security and identification in a global perspective*. London/New York: Routledge: 112-127.

Metropolitan Police (2016) Notting Hill Carnival 2016. Available at http://news.met.police.uk/news/notting-hill-carnival-2016-181523 (accessed 1 December 2016).

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

Mordini, Emilio and Sonia Massari (2008) Body, biometrics and identity, *Bioethics* 22(9): 488-498.

Muller, Benjamin J. (2004) '(Dis)Qualified Bodies: Securitization, Citizenship and 'Identity Management'', *Citizenship Studies* 8(3): 279–94.

National Research Council (2010) *Biometric Recognition: Challenges and Opportunities*. Washington, DC: The National Academies Press. doi: 10.17226/12720.

Norris, C. Moran, J. and G. Armstrong (eds) (1998) Algorithmic Surveillance: The Future of Automated Visual Surveillance' in *Surveillance, Closed Circuit Television and Social Control. Aldershot*, Ashgate. 255-276.

Novas, Carlos and Nikolas Rose (2000) Genetic Risk and the Birth of the Somatic Individual, *Economy and Society* 29(4): 485–513.

O'Gorman, Lawrence (1999) Fingerprint verification, in A. Jain et al (eds) *Biometrics: Personal Identification in Networked Society*. Kluwer Press: Dordrecht.

Privacy International et al. (2004) *Open letter to the European Parliament on biometric registration of all EU citizens and residents*. [online] Available at: https://www.privacyinternational.org/node/269 (Accessed 30 November 2016).

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

Ramanathan, Usha (2010) The Personal is the Personal. *Indian Express* (Delhi, January 6, 2010, Available at http://www.indianexpress.com/news/the- personal-is-the-personal/563920/0 (accessed 10 February 2011).

Shukla, Ravi (2010) Reimagining citizenship: Debating India's Unique Identification Scheme, *Economic and Political Weekly*, XLV(2): 31-36.

Statewatch (2003) *Biometrics - the EU takes another step down the road to 1984*. [online] Available at: http://www.statewatch.org/news/2003/sep/19eubiometric.htm (accessed 30 November 2016).

Statewatch (2004a) *European Parliament's Committee on Citizens' Freedoms and Rights delays its report on EU biometric passports until the autumn*. [online]. Available at: http://database.statewatch.org/article.asp?aid=25500 (Accessed 30 November 2016).

Statewatch (2004b) *EU governments blackmail European Parliament into quick adoption of its report on biometric passports*. [online] Available at: http://www.statewatch.org/news/2004/nov/12biometric-passports-blackmail.htm (Accessed 30 November 2016)

The Irish Council for Bioethics (2009) *Biometrics: Enhancing Security or Invading Privacy*. Dublin: Irish Council for Bioethics.

UIDAI (2010) *UIDAI Strategy Overview. Creating a Unique Identity Number for every Resident in India.* New Delhi: Unique Identification Authority of India, Planning Commission.

UK House of Commons (2015) *Current and future uses of biometric data and technologies*. Science and Technology Committee. Available at: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf

UNHCR (2012) An efficient and protective EURODAC. Available at http://www.unhcr.org/50adf9749.pdf (accessed 25 November 2016)

van der Ploeg, Irma (2003) Biometrics and Privacy: A note on the politics of theorizing technology, *Information, Communication & Society* 6(1): 85-104.

van der Ploeg, Irma (2009) Machine-readable bodies: biometrics, informatisation and surveillance in Emilio Mordini and M Green (eds) *Identity, Security and Democracy: Social, Ethical and Policy Implications of Automated Systems for Human Identification*, IOS Press, NATO Science Series: Human and Societal Dynamics, 49: 85-94.

Wood, David Murakami and Stephen Graham (2014) Permeable Boundaries in the Software-Sorted Society: Surveillance and Differentiations of Mobility, in Mimi Scheller and John Urry (eds) *Mobile Technologies of the City*, Routledge, London

World Bank (2015) Identification for Development (ID4D). Integration Approach. Washington: The International Bank for Reconstruction and Development/ The World Bank Group.

Zwitter, Andrej (2015) Big Data and International Relations, *Ethics and International Affairs* 34(4): 377-389.

## Suggestions for further reading

**European/National Parliament reports on biometrics**

European Agency for the operational management of Large-Scale IT Systems, "Biometrics in Large-Scale IT: Recent trends, current performance capabilities, recommendations for the near future", 2015. http://www.eulisa.europa.eu/Publications/Reports/Biometrics%20in%20Large-Scale%20IT.pdf

European Biometrics Forum, "Security & Privacy in Large Scale Biometric Systems", 2006. http://is.jrc.ec.europa.eu/documents/SecurityPrivacyFinalReport.pdf

European Biometrics Portal, "Biometrics in Europe – Trend Report", 2007. http://staatswissenschaft.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/21063courseWebsite/Biometric-TrendReport2007.pdf

European Commission Institute for Prospective Technological Studies, "Biometrics at the Frontiers: Assessing the Impact on Society", 2005. http://ftp.jrc.es/EURdoc/eur21585en.pdf

European Commission Joint Research Centre, "Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats", 2008.

European Commission Joint Research Centre, "Fingerprint Recognition for Children", 2013. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20(pdf).pdf

European Commission Joint Research Centre, "Fingerprint identification technology for its implementation in the Schengen Information System II (SIS - II)", 2015. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97779/lbna27473enn.pdf

European Commission Privacy and Emerging Sciences and Technologies research project, "Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment". 2011. http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf

Italian Istituto Superiore di Sanità (National Institute of Health), "Ethical and social implications of biometric identification technology", 2007. http://www.iss.it/binary/publ/cont/STAMPA%20ANN_07_02%20Mordini.1180428288.pdf

Tilburg University for the Council of Europe, "Report on the application of the principles of Convention 108 to the collection and processing of biometric data", 2013. https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CoE_Progress_report_2013%2004%2012_17%2046_final!.pdf

UK Commissioner for the Retention and use of Biometric Material, "Annual report 2014", 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387601/45428_Biometrics_Annual_Report_ACCESSIBLE.PDF

UK Commissioner for the Retention and use of Biometric Material, "Annual report 2015", 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/507104/54496_Biometrics_Commissioners_Report_Print_Ready__3_.pdf

UK Commissioner for the Retention and use of Biometric Material, "Further report by the Biometrics Commissioner on issues raised in his 2015 annual report", 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526232/55843_BC_Report_ACCESSIBLE_01.pdf

UK House of Commons Science and Technology Committee, "Current and future uses of biometric data and technologies", 2015. http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf

European Union Agency for Fundamental Rights, "Fundamental rights implications of the obligation to provide fingerprints for Eurodac", 2015. http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-fingerprinting-focus-paper_en.pdf

European Union Agency for Fundamental Rights, "Fundamental Rights Report 2016", 2016. http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-fundamental-rights-report-2016-2_en.pdf

UN International Telecommunication Union – Technology Watch, "Biometrics and Standards", 2009. http://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002PDFE.pdf

Organisation for Economic Co-operation and Development, "Background material on biometrics and enhanced network systems for the security of international travel", 2004. http://www.oecd.org/internet/ieconomy/34661198.pdf

**NGO reports**

Big Brother Watch, "Biometrics in Schools: The extent of Biometrics in English secondary schools and academies", 2014. https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf

Cato Institute, "Human Bar Code: Monitoring Biometric Technologies in a Free Society", 2002. http://object.cato.org/sites/cato.org/files/pubs/pdf/pa452.pdf

Forensic Science Special Interest Group, "Fingerprinting – the UK landscape: Processes, Stakeholders and Interactions", 2015. https://connect.innovateuk.org/documents/3144739/11337151/Fingerprinting+the+UK+Landscape+2015/57b0ea59-00ef-4818-801b-3e844ad21a6b

Genewatch UK, "Parliamentary vote on the Prüm Decisions: Sharing DNA profiles and fingerprints across the EU requires further safeguards", 2015. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/Pruembrief_Nov15_fin.pdf

Liberty, "Overlooked: Surveillance and personal privacy in modern Britain", 2007. https://www.liberty-human-rights.org.uk/sites/default/files/overlooked-privacy-report-december-2007.pdf

Liberty, "Liberty's response to the Human Genetic Commission's Consultation on the National DNA Database", 2008. https://www.liberty-human-rights.org.uk/sites/default/files/response-to-consultation-on-national-dna-database.pdf

Liberty, "Liberty's response to the Home Office's Consultation: Keeping the Right People on the DNA Database: Science and Public Protection", 2009. https://www.liberty-human-rights.org.uk/sites/default/files/liberty-s-response-to-dna-database-consultation.pdf

**Ethics**

Irish Council for Bioethics, "Biometrics: enhancing security or invading privacy?", 2009. http://irishpatients.ie/news/wp-content/uploads/2012/04/Irish-Council-Bioethics-Final_Biometrics_Doc_HighRes.pdf

Nuffield Council on Bioethics, "The forensic use of bioinformation: ethical issues", 2007. http://nuffieldbioethics.org/wp-content/uploads/The-forensic-use-of-bioinformation-ethical-issues.pdf

UK Metropolitan Police Authority Civil Liberties Panel, "Protecting the innocent: The London experience of DNA and the National DNA Database", 2011. http://policeauthority.org/metropolitan/downloads/scrutinites/dna.pdf

UK National DNA Database Ethics Group, "Sixth annual report of The Ethics Group: National DNA Database", 2013. https://www.gov.uk/government/publications/ndnad-ethics-group-6th-annual-report-2013

UK National DNA Database Ethics Group, "Seventh annual report of The Ethics Group: National DNA Database", 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415342/2903782_NDNADatabase_EG_AR_2014_acc.pdf

***Academic sources*:**

**Ethics of biometrics**

Alterman, Anton. "'A piece of yourself': Ethical issues in biometric identification". *Ethics and Information Technology Journal*. 2003.

Ashbourn, Julian. "The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies". *Background paper for the Institute of Prospective Technological Studies, DG JRC - Sevilla, European Commission*. 2005.

Brey, Philip. “Ethical Aspects of Facial Recognition Systems in Public Places.” *Journal of Information, Communication & Ethics in Society*. 2004.

Chinchilla, Rigoberto. “Ethical and social consequences of biometric technologies”, 2011.

Cho, Mildred K, and Pamela Sankar, “Forensic genetics and ethical, legal and social implications beyond the clinic”. *Nature Genetics*. 2004.

Davies, Simon. *Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine*. 1994.

Haimes, Erica. “Social and ethical issues in the use of familial searching in forensic investigations: insights from family and kinship studies.” *The Journal of Law, Medicine & Ethics*. 2006.

Lodge, Juliet. “The Dark Side of the Moon: Accountability, Ethics and New Biometrics.” *Second Generation Biometrics: The Ethical, Legal and Social Context*. 2012.

Mordini, Emilio and Corinna Ottolini. “Body identification, biometrics and medicine: ethical and social considerations.” *Annali dell'Istituto Superiore di Sanità*. 2007.

Schumacher, Günter. “Behavioural Biometrics: Emerging Trends and Ethical Risks.” *Second Generation Biometrics: The Ethical, Legal and Social Context*. 2012.

Sprokkereef, AnneMarie and Paul de Hert. “Ethical practice in the use of biometric identifiers within the EU”. *Law, Science and Policy*. 2007.

Toom, Victor, Matthias Wienroth, Amade M’charek, Barbara Prainsack, Robin Williams, Troy Duster, Torsten Heinemann, Corinna Kruse, Helena Machado, and Erin Murphy. “Approaching ethical, legal and social issues of emerging forensic DNA phenotyping (FDP) technologies comprehensively: Reply to 'Forensic DNA phenotyping: Predicting human appearance from crime scene material for investigative purposes' by Manfred Kayser.” *Forensic Science International: Genetics*. 2016.

Van Schomberg, Ralph. “From the Ethics of Technology towards an Ethics of Knowledge Policy and Knowledge Assessment.” Governance and Ethics Unit of dG Research, European Commission. 2007.

Wickins, Jeremy. “The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification”. *Science and Engineering Ethics*. 2007.

Wienroth, Matthias, Niels Morling, and Robin Williams. “Technological Innovations in Forensic Genetics: Social, Legal and Ethical Aspects”. *Recent Advances in DNA and Gene Sequences*. 2014.

Woodward, John, Katharine Watkins Webb, Elaine Newton, Melissa Bradley, David Rubenson, Kristina Larson, Jacob Lilly, Katie Smythe, Brian Houghton, Harold Alan Pincus, Jonathan Schachter, and Paul Steinberg. *Army Biometric Applications Identifying and Addressing Sociocultural Concerns*. 2001.

**Politics of biometrics**

Jacobsen, Katja Lindskov. *The politics of humanitarian technology: good intentions, unintended consequences and insecurity*. London: Routledge. 2015.

Sprokkereef, AnneMarie and Paul de Hert. "The EU and interoperability: Biometrics as a primary key". *Future of Identity in the Information Society*. 2007.

van der Ploeg, Irma. "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification." *Ethics and Information Technology*. 1999.

Zureik, Elia and Karen Hindle. "Governance, Security and Technology: The case of biometrics." *Studies in Political Economy*. 2004.

**Biometrics and human rights [including privacy]**

Bringer, Julien and Hervé Chabanne. "Two Efficient Architectures for Handling Biometric Data While Taking Care of Their Privacy". *Security and Privacy in Biometrics*. 2013.

Bustard, John. "The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications." *IEEE Signal Processing Magazine*. 2015.

Campisi, Patrizio. "Security and Privacy in Biometrics: Towards a Holistic Approach". *Security and Privacy in Biometrics*. 2013.

Cavoukian, Ann, Tom Marinelli, Alex Stoianov, Karl Martin, Konstantinos N. Plataniotis, Michelle Chibba, Les DeSouza, and Soren Frederiksen. "Biometric Encryption: Creating a Privacy-Preserving 'Watch-List' Facial Recognition System". *Security and Privacy in Biometrics*. 2013.

Crompton, Malcolm. *"Biometrics and Privacy the End of the World as We Know it or the White Knight of Privacy?" Australian Journal of Forensic* Sciences. 2004.

de Hert, Paul. "Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions". *Security and Privacy in Biometrics*. 2013.

de Hert, Paul and Annemarie Sprokkereef. "Biometrics, Privacy and Agency". *Second Generation Biometrics: The Ethical, Legal and Social Context*. 2012.

Freeman, Edward. "Biometrics, evidence and personal privacy." *Information Systems Security*. 2003.

Kindt, Els. "Best Practices for Privacy and Data Protection for the Processing of Biometric Data". *Security and Privacy in Biometrics*. 2013.

Koops, Bert-Japp and Annemarie Sprokkereef. "Biometrics: PET or PIT?" *Future of Identity in the Information Society.* 2009.

Ratha, Nalini, Jonathan Connell, and Ruud Bolle. "Enhancing security and privacy in biometrics-based authentication systems." *IBM Systems Journal*. 2001.

Sanchez-Reillo, Raul, Raul Alonso-Moreno, and Judith Liu-Jimenez. "Smart Cards to Enhance Security and Privacy in Biometrics". *Security and Privacy in Biometrics*. 2013.

Steward, Blair. "Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies." *Privacy Law & Policy Reporter*. 1999.

Thomas, Rebekah. "Biometrics, international migrants and human rights." *European Journal of Migration and Law*. 2005.

Tilton, Catherine J. and Matthew Young. "Standards for Biometric Data Protection". *Security and Privacy in Biometrics*. 2013.

Topfer, Eric. *"Network with errors": Europe's emerging web of DNA databases.* Statewatch analysis, 2011.

van der Ploeg, Irma. "Biometrics and Privacy: A note on the politics of theorizing technology." *Information, Communication & Society*. 2003.

Yue Liu, Nancy. *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*. 2011.

**Biometrics and law**

de Hert, Paul. "Biometrics: legal issues and implications". *Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission*. 2005.

de Hert, Paul and Annemarie Sprokkereef. "The privacy legal framework for biometrics: The Netherlands". *Future of Identity in the Information Society*. 2009.

de Hert, Paul, Wim Jan Schreurs and Evelien Brouwer. "Machine-readable identity documents with biometric data in the EU: Overview of the legal framework." *Keesing Journal of Documents*. 2007.

Kindt, Els. *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. 2013.

Kindt, Els. *The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective*. 2014.

Peers, Steve. *Biometric data and data protection law: the CJEU loses the plot*. Statewatch analysis, 2015.

Prins, Corien. "Making our bodies work for us: legal implications of biometric technologies." *Computer Law & Security Report*. 1998.

Sprokkereef, Annemarie. *"Data Protection and the Use of Biometric Data in the EU." Future of Identity in the Information Society*. 2007.

Sprokkereef, Annemarie and Suad Cehajic. "The privacy legal framework for biometrics: Germany". *Future of Identity in the Information Society*. 2009.

Sprokkereef, Annemarie and Suad Cehajic. “The privacy legal framework for biometrics: United Kingdom”. *Future of Identity in the Information Society*. 2009.

Yue Liu, Nancy. “Identifying Legal Concerns in the Biometric Context.” *Journal of International Commercial Law and Technology*. 2008.

**Biometrics and borders**

Lodge, Juliet. “eJustice, Security and Biometrics: the EU's Proximity Paradox.” *European Journal of Crime, Criminal Law and Criminal Justice*. 2005.

Lodge, Juliet and Annemarie Sprokkereef. “Accountable and transparent e-security: The case of British (in) security, borders and biometrics.” *Challenge*. 2009.

Jeandesboz, Julien, Jorrit Rijpma and Didier Bigo (2016) *Smart Borders Revisited: An assessment of the Commission’s revised Smart Borders proposal*. Study for the LIBE Committee, European Parliament. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU(2016)571381_EN.pdf

**Biometrics and identity**

Spinello, Richard and Herman Tavani. “Biometrics and Identity.” *Reading in Cyberethics*. 2004.

Sprokkereef, Annemarie. “Identity in the Information Society: Exploring Legal Approaches to the Use of Biometric Data”. 2007.

Schouten, Ben, Albert Salah, and Rob van Kranenburg. “Behavioural Biometrics and Human Identity.” *Second Generation Biometrics: The Ethical, Legal and Social Context*. 2012.

Solove, Daniel. “The Digital Person and the Future of Privacy.” *Privacy and Technologies of Identity - A Cross-Disciplinary Conversation*. 2006.