Project	**MobilePass**
Project Reference:	Grant agreement no. 608016
Project Short Name:	MobilePass
Call:	FP7-SEC-2013-3-2-3
Funding Scheme:	Capacity Project
Project web-site:	www.mobilepass-project.eu

Deliverable 2.1
Implications of Biometrics-based Mobile Border Control - Preliminary

Document			
Deliverable No.:	2.1	Due Date:	2015-28-02
Issued by Partner:	UNU-MERIT	Actual Date:	2015-28-02
WP/Task:	WP2/T2.1	Pages:	XX
Confidentiality Status:	PU		

Authors	**Name**	**Organization/Unit**
Author	Sanneke Kloppenburg	UNU-MERIT
	Irma van der Ploeg	UNU-MERIT

Authorization	**Name**	**Organization/Unit**
Project Officer	Andrei Lintú	European Commission

Table of Content

Introduction

Mobile biometric border control

Identification systems provide the basis for the interaction of individuals with states and non-state organisations. Verifying an individual's identity is crucial for determining their access to rights and services, such as social security, border crossing, and financial services. Biometric identification is claimed to be a more reliable means of identification than traditional paper-based forms and is increasingly used in countries all over the world. One area in which biometric technologies are being adopted at a large-scale is the management of Europe's external borders. Over the past 10 years, several large-scale biometric databases for the purposes of border control in the service of migration and mobility management have been introduced, and since October 2014, the biometric verification of visa holders at the external border is mandatory. At airports, we are witnessing a trend to introduce automated biometric border control for European citizens in possession of an e-passport. One of the main rationales behind this is that the use of biometrics would improve both the security and efficiency of border crossing.

These developments, in combination with increasing traveller flows at the external border, have led to a demand for new technological equipment for conducting biometric traveller verification and identification at land borders. Mobile equipment would allow border authorities to conduct biometric verification of travellers in places away from the fixed border crossing points, for example inside vehicles and trains. This is expected to enhance both the security and efficiency of land border crossing-points.

Purpose and scope

The purpose of the MobilePass project is to design, develop, and demonstrate technologically advanced mobile equipment that enable border control authorities to perform full page passport scanning and biometric identification of travellers at land borders. One of the more specific goals of the project is to develop new technologies of video-based face recognition technologies and contactless fingerprint recognition technologies. Within the MobilePass project, one work package (WP2) is dedicated to investigating the social, ethical, and legal issues potentially arising from its research and from the application of the solutions it aims to develop. Paying attention to social, ethical and legal aspects already in the design phase contributes to the responsible development and implementation of biometrics-based mobile border control.

The purpose of this Deliverable (D2.1) is to identify legal, social, and ethical challenges raised by mobile biometric border control. It takes as a starting point the vision of future mobile biometric devices and the user requirements as developed by technical project partners (in Deliverables 1.1 and 1.3). The analysis of legal, social, and ethical issues in this Deliverable also forms the basis for Deliverable 2.2, in which we develop guidelines for responsible design and use of mobile biometric devices. 'Responsibility' in designing and implementing biometric systems starts with understanding how, when and for whom the affordances of biometric systems have (potentially) undesirable effects.

Outline

This report starts with a short description of the workings of biometric technologies in order to provide readers who do not have a background in biometrics with a basic understanding of the process of biometric recognition, and the main terms used in the field of biometric sciences.

Part I of this report discusses the legal aspects of mobile biometric border control at the external European borders. It first describes the existing legal framework for data protection, privacy and fundamental rights at European level. Next, it discusses the European legal framework for (biometric) border control.

In Part II we discuss social and ethical aspects of mobile biometric border control. We focus on three issues in particular: first, we discuss how the process of biometric recognition itself and the specific technologies constituting it bring along social and ethical issues. Second, we discuss how biometric systems afford (new) information processing practices that carry specific risks. Third, we discuss the ethical and social challenges connected to the *mobile, or portable* character of mobile biometric devices for border control.

1. How biometric systems work

1.1 Introduction

Before elaborating on the legal, social and ethical aspects of mobile biometric border control, we first we want to take a step back to describe how biometric systems work and introduce the main terms and concepts used in the biometrics industry and literature.

1.2 Biometric systems

A biometric system measures one or more physical or behavioural characteristics of an individual to determine or verify his identity (Jain et al 2011, p. 3-4). This is a process that consists of several steps. First, a person needs to *enrol* in a biometric system: a sensor device captures a digital representation of a unique physical characteristic of an individual (e.g. fingerprints, iris, face) and this digital representation, the *captured biometric sample* (sometimes also called the raw biometric data), is transformed via algorithms into a *biometric template.* This template consists of only the relevant information that is needed for recognising the person (a *feature set*), and this information is said to be irreversible, meaning that the biometric characteristic itself cannot be deduced from the template. The biometric template is stored in a database or on a token (e.g. a chip on a smart card), together with some identifying information of the person (e.g. a name, visa number). In the recognition phase, a sensor device again captures a digital representation of the person's biometric characteristic. The biometric system transforms the biometric sample via algorithms into a new feature set, the *biometric probe*, and compares these features against the features of the stored template(s) to generate comparison scores. These *comparison scores* indicate how alike the biometric probe and biometric template are. If the comparison score is above a specific *threshold,* the person presenting herself is 'recognised' by the system (Jain et al 2011).

1.3 Biometric recognition

Biometric recognition is the automated recognition of individuals based on their biological and behavioural characteristics (ISO ISO/IEC 2382-37) and encompasses verification and identification. In *verification*, an biometric probe is compared to a stored template that corresponds to the claimed identity (a one-to-one match). Hence, a person 'claims an identity and the system verifies whether the claim is genuine, i.e., the system answers the question "Are you who you say you are?" (Jain et al 2011). An example of this is when a traveller presents herself at a border checkpoint where her fingerprints are scanned and the produced biometric probe is compared to the stored template in the chip on her passport. After comparing the two feature sets, the system produces a comparison score. If the comparison score, or match score, is similar to or higher than a pre-defined threshold, the identity claim is accepted as genuine. In practice, the comparison score can never be 100%, due to variances in the acquired samples of a biometric characteristic of a person, something we will come back later.

In *identification*, the system compares an biometric probe to a database containing many different templates (a one-to-many match). Here the question "Are you someone who is known to the system?" is answered (Jain et al 2011)?". An example of this is the identification of people who the authorities suspect of illegally staying in an EU member state by checking their fingerprints against the Eurodac database in which the fingerprints of asylum applicants are stored. Again, by comparing a biometric probe with all templates stored in a particular database, the system produces comparison scores. The comparison scores that are equal to or above the threshold can be sorted from highest to lowest, and the system may for example output either the identity of the person whose template has the highest comparison score or a rank list of possible matches. Of course the system can also output that the person was not found in the database (i.e. the comparison scores were below the set threshold).

1.4 Biometric system errors

In the biometrics literature, several types of errors and problems of biometric systems are distinguished, among which failure to capture, failure to enrol, false accept rate, and false reject rate. A *failure to capture* occurs when 'a particular sample provided by the user during authentication cannot be acquired or processed reliably. The *failure to enrol rate* (FTE) refers to 'the proportion of users that cannot be successfully enrolled in a biometric system' (Jain et al 2011, p. 22.) A false acceptance happens when the system incorrectly identifies a person, or fails to identify an imposter. A false rejection happens when the system fails to verify/identify an authorised person. The *false accept rate* (FAR) is 'the fraction of impostor scores that are greater than or equal to the threshold (n)' and the *false reject rate* (FRR) denotes 'the proportion of genuine scores that are less than the threshold (n) (Jain et al 2011, p. 18). Both the FAR and FRR depend on the threshold. This means that if the threshold is increased, the FAR will decrease, but at the same time the FRR will increase. Similarly, if for a particular biometric system the threshold is lowered, the FRR will decrease , but the FAR will increase. Hence, it is never possible to simultaneously decrease the FAR and the FRR by adjusting the threshold in a particular biometric system.

Because the threshold of a biometric system can be adjusted, the system can be operated to produce different levels of FAR/FRR. The Detection Error Tradeoff Curve (DET curve) plots the FAR against the FRR at various thresholds. This allows for a theoretical comparison of the accuracy of different systems (e.g. comparing the FAR of two different systems for the same FRR). However, the actual system performance depends on many different factors such as the quality of the biometric sample, the quality of algorithms, and the quality of the reference template(s). When a biometric sample is acquired, the quality of the image is influenced by environmental factors such as temperature, lighting, humidity, by the 'quality' of the biometric characteristic (damaged fingerprints), and by user interaction with the capturing device (position of the finger, rotation of the face etc). Because factors such as lighting, pose, and humidity vary with each scan or image, this results in variability in the biometric feature set of an individual ('intra-class variations'/intra-user variations). When features are extracted from the captured image and biometric feature sets are compared, a lot depends on the quality of the algorithm (the range of conditions/user population characteristics it can perform well with), the size of the biometric reference database for identification (the larger the database, the more errors occur) and the quality of templates (e.g. due to *template ageing*).

Part I

Legal aspects of mobile biometric border control

The first part of this report discusses the legal aspects of biometric border control at the external European borders. It describes the existing legal frameworks at European level for data protection, privacy and fundamental rights and for (biometric) border control.

It is important to understand the legal context of biometric border control for two reasons. First, the mobile biometric device that is going to be developed in the MobilePass project *must comply with the existing rules and standards*. Second, new developments in (biometric) technologies, or new ways of using such technologies, may not be covered by the existing legal framework or bring with it *issues that require new or additional rules and standards*.

Both the management of the external borders and the protection of personal data are *highly dynamic policy areas*. The EU seeks to make border management more efficient by implementing new technologies and systems for border control, including the use of biometrics. It promotes the use of automated border control for EU citizens and has issued proposals to 'speed-up, facilitate and reinforce' border check procedures for foreigners travelling to the EU. The European framework for data protection is also under discussion, with a new proposal for a Data Protection Regulation awaiting adoption by the Council. This means that the current legal framework for mobile biometric border control is subject to change. The chapters will therefore, where possible, also discuss the relevant expected changes.

In discussing the legal aspects of biometric border control, the chapters below take as its point of the departure the MobilePass device base line scenario as developed in D1.1 and D1.3. In this scenario, the MobilePass device is a handheld device operated by a border guard and performs the following functions: document authentication, biometric verification (fingerprints and face), and background checks. The MobilePass device is primarily being used for the purposes of carrying out border checks on EU citizens and third country nationals at land border check points at the external border of the European Union. These border checks may take place inside cars, buses, and trains.

2. Biometric data, data protection, and fundamental rights in the European Union

The future MobilePass device will be processing personal data (passport data, fingerprints and facial images). **Directive 95/46/EC governs the processing of personal data within the European Union**. In section 2.1 we discuss the relevant articles of the Data Protection Directive. Because the Directive will be replaced by a Data Protection Regulation in the near future, we shortly discuss the relevant changes this will introduce for the processing of biometric data. In section 2.3, we discuss how the processing of biometric data relates to the **fundamental rights of data subjects**. With the entry into force of the Lisbon Treaty[1] in 2009, **fundamental rights -including the right to respect for privacy and data protection- were incorporated in Union law, which means they are now legally binding**.

2.1 Directive 95/46/EC

The European Data Protection Directive (Directive 95/46/EC) constitutes the main legal framework for the processing of personal data within the European Union. The Data Protection Directive defines *personal data* as 'any information relating to an identified or identifiable natural person'. An *identifiable person* 'is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.' **Biometric data, by their very nature, always relate to an identifiable individual, and hence should be considered personal data** (Article 29 WP80). It should be noted that the data protection principles in the Directive do not explicitly deal with the processing of *biometric* data. Several bodies, among which the Article 29 Working Party[2], have issued opinions in which more detailed, but non-binding, guidelines and recommendations on the processing of biometric data are provided.

The definition of *data processing* is a very broad one, covering 'any operation or set of operations which is performed upon personal data, whether or not by automatic means', and includes 'collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction' (Directive 95/46/EC). **This means that several of the operations to be performed by the MobilePass device for traveller identification are forms of personal data processing.**

The *scope* of the Directive however is limited. The Directive does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security […] and the activities of the State in areas of criminal law (art3(2)). Over the years, however, more and more policy areas have become incorporated in Community law, and in principle the Directive now covers the areas of external border control, visas, immigration and asylum (see De Hert & Riehle 2010). An exception would be those border check practices that are based on criminal law, such as searches in police databases[3].

2.1.1 Fair and lawful processing

Article 6(a) of the Directive 95/46/EC specifies that personal data must be processed fairly and lawfully.

2.1.2 Purpose limitation

Article 6(b) directs that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (art 6(b). This is called the *principle of*

[1] The Treaty of Lisbon amended the two treaties which form the constitutional basis of the European Union: the Treaty on European Union and the Treaty establishing the European Community.

[2] The Article 29 Data Protection Working Party is an independent European advisory body and was set up under the Directive 95/46/EC. It has advisory status and acts independently.

[3] The processing of personal data in the framework of police and judicial co-operation in criminal matters is protected under Framework Decision 2008/977/JHA, Council of Europe Convention 108, and Police Recommendation R (87) 15..

purpose limitation, or *purpose specification.* The Article 29 Working Party (WP 193, p. 7) has stressed that because the processing of biometric data carries risks related to the protection of fundamental rights and freedoms of individuals, there needs to be a clear definition of the purpose for which the biometric data are collected and processed.

2.1.3 Proportionality

In addition, the Directive stipulates that data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (art 6(c)). In other words, the data processing must be *proportional* to the pursued (legitimate) goal. The Article 29 Working Party has specified four factors to take into account when analysing the proportionality of a proposed biometric system (WP 193).

The first factor is whether the biometric system is *necessary* to meet the *identified need.* The identified need to which the MobilePass device would contribute is securing, facilitating and speeding up border passage of travellers (European and from third countries) at the external borders of the EU. Biometric verification is generally understood as being more reliable than manual verification (and hence raising the security level) and automating (parts of) the border control process would save time and resources. Whether or not these aims are achieved in practice depends on many factors[4].

The second factor is whether 'the system is likely to be *effective* in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used' (WP193). The two biometric modes used in the MobilePass device (face and fingerprint) are standard modes[5] used in e-passports and in border control and in that sense could be considered appropriate. The envisioned MobilePass device will use contactless fingerprint capture and advanced mobile facial capture with the aim of 'increasing security (e.g. minimise spoofing and evasion) while making the control less cumbersome for passengers' (MobilePass Description of Work). Here, two important considerations are whether the remote capturing of biometrics could potentially decrease the accuracy of the biometric data and in what cases remote capturing may potentially violate the principle of fair processing (e.g. when people are unaware that their biometrics are being captured).

The third aspect to take into account when considering proportionality is whether the loss of privacy is proportional to any *anticipated benefit*. If, for example, the MobilePass device only causes a slight increase in convenience and/or security (or in a negative scenario even a decrease), the loss of privacy of travellers can be considered inappropriate.

The fourth aspect to weigh is whether the same goal could also be achieved with *less intrusive means*. This is of particular importance when the MobilePass device is used on travellers for whom biometric verification is currently not obligatory by law (European and visa-exempt travellers, see also Chapter 3). Could the same goal also be achieved by manual verification?

[4] As the Article 29 Working Party has argued, the use of biometrics per se does not ensure enhanced security. Some biometric data can be collected without the knowledge of the concerned person, thereby decreasing security, and biometric databases can potentially be hacked.

[5] ICAO (International Civil Aviation Association) recommends the face as 'the primary biometric, mandatory for global interoperability in passport inspection systems', while recommending finger and iris as 'secondary biometrics to be used at the discretion of the passport-issuing State' (ICAO 2006, p. 1). The European e-passport Regulation (Regulation (EC) No 2252/2004) directs the inclusion of the facial image and two fingerprints of the holder in passports and travel documents.

2.1.4 Data minimization

Related to the principle of proportionality is the *data minimisation principle*, which entails that only those data that are required to achieve the specified goal are processed, and not more. If too many data or irrelevant data are processed, the data may be excessive in relation to the purpose for which they are processed. The Article 29 Working Party called attention to the fact that biometric data often contain more information than is needed to perform verification or identification (see also section 7.3 of this Deliverable). Data minimisation in biometric systems is therefore a challenging obligation.

2.1.5 Data accuracy

Article 6(d) directs that data shall be accurate and, where necessary, kept up to date. It also stipulates that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. In relation to this article, it is important to stress that biometric data are never 100% accurate, as the capturing of a biometric is influenced by many factors, such as environmental conditions and pose and behaviour of the data subject. In addition, people's physical characteristics change over time due to, for example, ageing, injuries, or diseases, and this may cause the biometric data that is stored in a database to be outdated (see Chapter 6 for more details).

2.1.6 Data retention

According to Article 6(e), biometric data needs to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. This places restrictions on the storage of biometric data in databases.

2.1.7 Criteria for legitimate processing

Article 7 of the Directive sets out the criteria for making data processing legitimate. Of relevance for the use of the future MobilePass device is that personal data may be processed only if the data subject has unambiguously given his consent (7(a)); if processing is necessary for compliance with a legal obligation to which the controller is subject 7(c)); or if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (7(e)). As Chapter 3 discusses, for some groups of travellers, biometric verification at the external border is compulsory under de Schengen Borders Code. For those groups of travellers for whom biometric verification is not an obligation under the Schengen Borders Code, however, the legitimacy of processing is less obvious. In order to make the processing of their biometric data legitimate, subjects would need to give their consent. At some European airports, for example, European travellers can opt between using an Automated Border Control gate that uses biometric verification and the conventional (manual) border control. In any case where there is no legal basis to do so, the systematic use of a device for biometric verification should be avoided.

2.1.8 Data controllers' responsibilities

Article 17 places obligations on the data controller to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing. This obligation is particularly important in the context of biometric data. If biometric data get stolen, the consequences for the victim are severe, because biometrics are unique identifiers which cannot be replaced (see also section 7.2).

2.1.9 Data subjects' rights

Articles 10 and 11 state that data subjects have a right to know about the processing and the use of the processed data. In addition, all data subjects are endowed with a right of access to the biometrical data and to obtain upon request rectification, erasure or blocking of data when the processing violates the provisions (e.g. incomplete or inaccurate nature of the data).

2.1.10 Biometric data as sensitive data

An (unresolved) question is whether biometric data should be considered a *special category of personal data* under Article 8. This article in principle prohibits the processing of personal data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. There are however exemptions, for example when the data subject has given consent, or when the processing is related to security measures. The Article 29 Working Party is of the opinion that digital facial images may in some specific cases be considered as a special category of personal data. This is for example the case if they are processed to derive special categories of data such as racial or ethnic origin or data concerning health (WP 192, p.4). In section 7.3 we discuss more elaborately how biometric data may be revealing of health information and information concerning racial or ethnic origin.

2.2 The draft EU General Data Protection Regulation

In 2012, The European Commission proposed *a new Data Protection Regulation that would replace Directive 95/46/EC*. As opposed to a Directive (in which Member States are required to achieve a particular result, but are free to choose the form and the means for applying the Directive), a Regulation is binding and directly applicable in all Member States. This means that with the new Regulation, a single set of rules about data protection that are valid across the EU will be implemented. The proposal is currently being discussed by the European Parliament and the Council of the EU, and the EC is aiming at an agreement by the end of 2015. The Regulation will apply from two years after its entry into force. We will discuss the implications of the relevant articles of the draft Regulations for MobilePass more elaborately in Deliverable 2.2. Below we provide a brief overview of the main points.

2.2.1 Data Protection Impact Assessment

Under Article 33 of the draft new Data Protection Regulation (COM 2012/0011), a data protection impact assessment (DPIA) will be required for processing operations that present 'specific risks to the rights and freedoms of data subjects'. **The processing of biometric data is one of the categories of processing that is mentioned as presenting such risks, and hence would require a DPIA.**

A DPIA would have to contain at least 'a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [the] Regulation' (art. 33(3)). An exception to the obligation to conduct a DPIA is made where the controller is a public authority or body and where the processing results from a legal obligation, but only in so far as the processing operations are regulated by European or national law and rules and procedures are provided for. This means that the processing of biometric data for identity checks at the external border, even if it would not require a DPIA, would still need to have a basis in law and be subject to specific rules and procedures.

2.2.2 Special categories of data

The proposed Regulation also contains an article on *special categories of data*, the processing of which is prohibited. Article 9 defines these special categories as data 'revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data or data concerning health or sex life or criminal convictions or related security measures'. Just like in the current Directive, **it is not explicitly mentioned if biometrics, or particular biometric modes, should be considered a special category of data**, so different interpretations will probably continue to exist here.

2.2.3 Consent

Whenever consent is required for data to be processed, it will have to be given *explicitly* (as opposed to 'passive consent'). The data controller has the burden of proving that the data subject has given the consent to the processing operations (art. 7).

2.2.4 Responsibilities of the controller

The draft Regulation introduces *increased responsibility and accountability for those processing personal data*. For example, each controller and processor is obliged to maintain documentation of all processing operations under its responsibility (art. 28).Controllers also need to implement appropriate technical and organisational measures, which include 'data protection by design and by default' (art. 23). In the case of a personal data breach, the controller needs to notify this to the supervisory authority, and in some cases also need to inform the data subject (art. 31 and 32). When controllers intentionally or negligently do not comply with the Regulation, the supervisory authority may impose a fine of up to 1.000.000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover (art. 79).

2.3 Biometrics and fundamental and human rights in the European Union

With the entry into force of the Treaty of Lisbon in 2009, **the Charter of Fundamental Rights of the European Union has become legally binding**. The Charter contains several articles that are relevant to the use of biometric data. Because the articles constitute legally binding fundamental rights, they apply to all policy areas, including the area of freedom, security and justice to which the management of the EU's external borders, visas, immigration and asylum belong.

2.3.1 Protection of personal data

Article 8 of the European Charter of Fundamental Rights (EUCFR) deals with the *protection of personal data*. It stipulates that:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.
>
> (EUCFR, art 8)

Hence, in addition to a general right to data protection, this article also provides persons with a right of access to their data, and a right to have it rectified.

In addition, the new Treaty on European Union (TEU) now contains a general provision on the right to data protection. Article 16 of the Treaty on the Functioning of the European Union (TFEU) asserts that '[e]veryone has the right to the protection of personal data concerning them'. Article 16(b) states that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data. This has resulted in the proposal for a new legal framework for data protection that would apply to almost all areas of the European Union[6].

2.3.2 Respect for private and family life

Article 7 of the EUCFR and Article 8(1) of **the European Convention on Human Rights (ECHR)** provide for *the right to respect for private and family life***.** In Article 8(2) of the ECHR, it is stated that '[t]here shall be no interference by a public authority with the exercise of this right *except such as is in accordance with the law and is necessary in a democratic society* [our emphasis.] *in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*'.

How does the use of biometrics relate to the right to privacy? On the one hand, biometrics can be seen as enhancing privacy because they allow the verification of identity without disclosing name address, or other personal data. On the other hand, biometrics can be seen as posing a threat to privacy, for example through misuse of information, identity theft, loss of control over one's biometric data, and profiling. We elaborate on these arguments in [the chapter on social and ethical aspects]. The European Court of Human Rights (ECtHR) has held in several cases that the *collecting, processing* and *retention* of fingerprints amounts to an interference with the right to privacy (see S and Marper vs the United Kingdom, 2008; M.K. vs France, 2013). The public authority that is processing biometric data needs to be able to show that 1. the interference serves a legitimate aim, 2. is in accordance with the law, and 3. is necessary in a democratic society. In the conclusion of this chapter we discuss what such an assessment could look like for the processing of biometric data within the MobilePass system.

2.3.3 Bodily integrity

The EUCFR also contains an article guaranteeing the right to physical integrity (art 3 EUCFR). This can be understood as the right to control over one's own body. While biometrics are sometimes understood as non-invasive because they do not require penetration of the body's surface (see e.g. Prins 1998), other viewpoints are that the capturing, storing and processing of body data touches upon the integrity of the body and the person, because this entails the monitoring, categorising, scrutinising and, ultimately, controlling and manipulating of persons through their bodies (Van der Ploeg 2005).

2.3.4 Equality and non-discrimination

Other relevant articles in the EUFCR are those that specify the *principle of equality*. The right to non-discrimination (art 21 EUCFR) entails that '[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'.

The relation of this principle to biometrics has two sides, rendering it rather ambivalent. One the one hand, biometrics may be considered as *contributing* to equal treatment of people. While border

[6] It would apply to all areas except for common foreign and security policy, which will remain subject to special rules (art 39 TEU). The Treaty also includes two declarations that provide derogations to Article 16 TFEU: Declaration 20 states that whenever rules on protection of personal data could have direct implications for national security, 'due account will have to be taken of the specific characteristics of the matter'. Declaration 21 emphasises that in the fields of judicial cooperation in criminal matters and police cooperation, specific rules on the protection of personal data and the free movement of such data 'may prove necessary because of the specific nature of these fields'**.**

guards may have preconceived judgements about individuals, biometric systems are generally understood as being 'neutral'.

On the other hand, biometric systems may *violate* the principle of equality in different ways: First, biometric technologies produce body data and this data can potentially allow for categorisation, which may result in discrimination. More specifically, research has shown that biometrics may reveal ethnic origin, and a problem stemming from this is that it can allow for automated ethnic classification. Second, studies have shown that biometric technologies may produce 'biased failures', which means that the technologies work worse with people of a certain ethnic background, age, or gender. This is related to several articles in the EUCFR guaranteeing the rights of particular groups of people, including:

- Respect for cultural, religious and linguistic diversity (art 22)
- Equality between women and men (art 23)
- Rights of the child (art 24)
- Rights of the elderly (art 25)
- Integration of persons with disabilities (art 26)

If particular (groups of) people experience problems in using biometric systems (for example when they are unable to use a biometric system due to their age or a physical handicap) this may violate *human dignity* and the ability for *equal participation* in society.

2.3.5 Right to freedom of movement and right to asylum

Other fundamental rights come into view when we consider *the mobile character of the MobilePass device*. Because the device will be a handheld biometric system with the capacity to connect to information systems, border authorities may carry the device with them and perform checks away from the regular border control points. In this way, the device potentially allows for the biometric border to 'materialise' in places away from the territorial border, including places *within* the European Union and places *outside* the territory of the EU. If border checks take place within the territory of the Member States without a legal basis[7], this may violate the right to freedom of movement and of residence within the territory of the Member States for citizens of the EU and legally resident Third County Nationals under article 45 of the EUCFR. In a similar way, if border checks take place outside the territory of the EU, for example at airports abroad or in extraterriotial waters, there is a danger that people's right to asylum (art. 18 EUCFR) is violated. It may lead to situations in which people they have never officially 'arrived' at the European border and hence cannot apply for asylum. The way in which the MobilePass device 'mobilises' the border is discussed in more detail in Chapter 8.

2.4 Preliminary conclusions

We can conclude that there is not one general legal framework in Europe governing the processing of *biometric data* as such. Because biometric data constitute personal data, their processing is regulated by the European Directive on Data Protection. In addition, the use of biometrics touches upon fundamental and human rights such as the right to data protection, privacy, physical integrity, and rights relating to equality, asylum and freedom of movement. We have seen that Article 6(a) of

[7] The Schengen Borders Code guarantees the free movement of EU citizens and qualified third-country nationals (TCNs) within the Schengen Area, but also allows Member States to temporarily reintroduce border control at internal borders in the event of a serious threat to their public policy or internal security.

the Directive underlines that personal data needs to be processed lawfully, and that the ECtHR stresses that because the use of biometrics constitutes an interference with privacy, it needs to have a legal basis. In the next chapter, we discuss *specific legislations* on European level on biometric border control to find out:

- Whether the use of biometrics in border control has a basis in law. Do the regulations explicitly mention the use of biometrics?
- If the legislation contains specific conditions and safeguards for the use of biometrics for border control purposes.

3. The legal basis of biometric border control

One of the functions that the future MobilePass device is to perform is the biometric verification of travellers' identities at the border. This chapter discusses the legal framework of biometric-based border control. The Schengen Borders Code provides the general framework for border control, whereas regulations on large-scale information systems such as SIS II, Eurodac, and VIS provide a legal basis for the processing of biometric data for specific purposes. Where the previous chapter discussed the legal framework for the *processing of personal data in general*, this chapter discusses to what extent the legislation related to e-passports, border control, visas, immigration and asylum contains additional provisions and safeguards on the *processing of biometric data*?

3.1 The Schengen Borders Code

The Schengen Borders Code (SBC) (Regulation No. 562/2006) sets out the rules governing the movement of people across the internal and external borders of the European Union (EU). With this regulation, border control at the so-called internal borders of the Schengen area has been abolished, while border control at the external borders has been strengthened. The Schengen Borders Code thereby guarantees the free movement of EU citizens and qualified third-country nationals (TCNs)[8] within the Schengen Area. Article 7 of the SBC lays down the rules for border checks of persons, clearly differentiating between EU citizens and third-country nationals (TCNs). When crossing the external Schengen borders, EU citizens[9] are to be subjected to a minimum check only, while third-country nationals undergo a more thorough check.

3.1.1 EU citizens

The procedure for a minimum check is described as follows:

[8] A third-country national is a person who is not an EU citizen. Regulation (EC) No. 539/2001 contains a list of Third Countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from the requirement.

[9] For reasons of simplicity, we use the term ‘EU citizens’ in this report when we want to refer to ‘persons enjoying the Community right of free movement’. Under the Schengen Borders Code, the following categories of persons enjoy the Community right of free movement: Union citizens and citizens of Iceland, Norway, Switzerland and Liechtenstein; third-country nationals who are members of the family of a Union citizen; and third-country nationals and their family members who, under agreements between the Community and its Member States, on the one hand, and those third countries, on the other hand, enjoy rights of free movement equivalent to those of Union citizens (Regulation No. 562/2006).

> 'All persons shall undergo a minimum check in order to establish their identities on the basis of the production or presentation of their travel documents. Such a minimum check shall consist of **a rapid and straightforward verification, where appropriate by using technical devices** [emphasis S.K.] and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting. (Regulation No. 562/2006, Art 7(2)).

On a non-systematic basis, border guards may, as part of the minimum check, also consult national and European databases in order to ensure that a person does not represent a threat to public policy, internal security, public health or the international relations of EU countries. **Article 7 does not explicitly mention the use of biometrics for verification. It does however state that technical devices may be used in the verification process.**

3.1.2 Third Country Nationals

Thorough checks for third-country nationals consist of a verification of the conditions governing entry[10], and, if applicable, of documents authorising residence and the pursuit of a professional activity (art 7(3)(a). The Schengen Borders Code was amended in 2009 (Regulation (EC) No 81/2009) and this amendment made the checking of visa holders against the Visa Information System (VIS) obligatory at entry and optional at exit. The use of live biometrics (fingerprints) of visa holders at the external borders for verification against VIS was first optional, but since October 2014 is obligatory at entry under the VIS Regulation (see section 3.3.2 on VIS below). **For third country nationals requiring a visa, the VIS Regulation and Schengen Borders Code thus allow (and make obligatory) systematic biometric verification against the VIS at entry.**

EU citizens	**TCNs**
Minimum check: a rapid and straightforward verification of the validity of the documents and a check for signs of falsification or counterfeiting	**Thorough check**: verification of the conditions governing entry, and, if applicable, of documents authorising residence and the pursuit of a professional activity
Database checks At entry and exit: *First line* -Document databases[11] (optional) -SIS II (non-systematic, verification using fingerprints optional) *Second line:*	**Database checks** At entry: *First line:* -Document databases (systematic) -SIS II (systematic, verification using fingerprints optional) -VIS (systematic, including obligatory biometric verification) *Second line:*

[10] In order to be allowed to stay on the territory of a Member States, third-country nationals must possess a valid travel document; possess a valid visa, if required; justify the purpose of his/her intended stay and have sufficient means of subsistence; not have an alert issued for him/her in the Schengen Information System (SIS) for the purpose of refusing entry; and not be considered a threat to public policy, internal security, public health or the international relations of EU countries (art. 5).

[11] Databases containing information concerning stolen, misappropriated, lost and invalidated documents.

-Verification against SIS II	-Identification against VIS using fingerprints allowed
	At exit: *First line* -Document databases (systematic) -SIS II (optional) -VIS (optional) *Second line:* -Identification against VIS using fingerprints allowed

3.2 Biometric verification using e-passports

The introduction of the e-passport made biometric verification of travellers at the external border possible. Another relevant development is that many Member States are introducing Automated Border Control using e-passports at airports. In this section we discuss to what extent these developments have led to rules or guidelines for processing the biometric data of travellers.

3.2.1 ICAO specifications for Machine Readable Travel Documents

At the external border, the travel documents of travellers form the basis for verifying their identity. Many countries now issue biometric passports. This enables the verification of live biometrics against the biometric reference image stored on a chip in the passport. The International Civil Aviation Organization (ICAO) has developed (non-binding) technical specifications for the incorporation of biometric identification in Machine Readable Travel Documents (MRTD). **The ICAO prescribes the storage of samples** 'to permit global interoperability'[12] (ICAO 2006, p.1).

3.2.2 Regulation on the European e-passports

In 2004, Regulation (EC) No 2252/2004 introduced the obligation for EU countries to issue e-passport containing biometrics. Since August 2006, digital facial images need to be included in passports and travel documents, and since June 2009 passports also need to contain two fingerprints. According to the European Council, the integration of biometric identifiers in travel documents makes the travel document 'more secure' and establishes 'a more reliable link between the holder and the passport and the travel document'. It would thereby make forgery and fraudulent use more difficult (Council Regulation (EC) No 2252/2004, p. 1).

The e-passport Regulation states that the biometric features will be stored on a storage medium in the passport or travel document (art. 1). In line with the ICAO specifications, *two fingerprints and facial image are stored in the form of sample images*. The e-passport Regulation does not allow the storing the fingerprints of the passport holder in other places than in the passport[13]. Furthermore, it directs that the biometric features stored in the passport will only be used for verifying 'the

[12] In the process of developing the specifications, the ICAO abandoned the concept of using templates 'due to the fact that templates and their readers are not internationally standardized' (ICAO 2006, p.1).

[13] The Netherlands, as the only country in the EU, did store the fingerprints of Dutch passport holders in a central database until 2011. In 2014, the Court of Justice in The Hague ruled that this storage was an unjustified violation of the right to privacy (Gerechtshof Den Haag, 18-02-2014). In 2013, the Court of Justice of the European Union ruled that the regulation 'does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone' (Case C-291/12 Michael Schwarz v Stadt Bochum, 17-10-2013)

authenticity of the document' (art. 4 (3)(a) and 'the identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law' (art. 4 (3)(b). **This means that while the e-passport Regulation governs the use of the biometric identifiers *that are stored on the RFID chip*, it does not cover the *capturing of live biometrics* of EU traveller and/or *the verification process as such* (i.e. the checking of live biometrics against the stored biometrics).** The latter two steps fall outside the scope of the regulation, and hence the Regulation does not provide a legal basis for conducting these steps in the verification process.

3.2.2 Automated Border Control for EU citizens

Despite the absence of specific provisions on the use of biometrics in the Schengen Borders Code, biometric verification of EU travellers at the external borders is already taking place as part of efforts to automate border control. The European Council views Automated Border Control (ABC) as a way to facilitate entry of EU citizens at the external borders. In a Council Conclusion of 2010, it invited Member States to move 'on voluntary basis to a more extensive use of automated border control systems on the basis of the new passport' as this would enable EU citizens to cross the external borders 'easily and quickly' (Council Conclusion 3 June 2010)[14]. Automated Border Control (ABC) is defined as 'the use of automated or semi-automated systems which can verify the identity of travellers at border crossing points (BCPs), without the need for human intervention' (Frontex 2012, p. 13). The rationale behind introducing automated border control is that it allows higher volumes of travellers to pass the first line checks (of the minimum checks) without having to increase the number of border guards. The border guards can then focus on checking higher risk travellers, and on the remaining manual checks.

An ABC system usually consists of one or more electronic gate(s), a document reader, a monitor and a biometric capture device. The traveller puts the data page of the passport on a document reader, which reads the Machine Readable Zone (MRZ), the data on the e-passport chip, and checks the optical security features of the passport to check whether the passport is valid and genuine. The live biometrics (face and/or fingerprints) of the traveller are captured and compared against the biometrics stored on the chip (facial image and/or fingerprints) in order to verify the identity of the traveller. On a random basis, a check may also be performed against national databases and the SIS. If these checks are successful, the traveller is allowed to cross the border. If the automated border control fails, the traveller is directed to the manual border control (Frontex 2012).

The process of Automated Border Control is not fully automated, but must always be supervised by a border guard. The border guard usually sits in a booth close to ABC systems to monitor the passengers, and the screen displaying the results of the verification processes in several e-gates. An important reason why ABC cannot be fully automated is that the Schengen Borders Code directs that *border guards* carry out checks on persons (art. 7(1)). Hence, ABC can only be implemented as a supporting technique and always needs to take place under the responsibility of border guards (Frontex 2012).

3.2.3 Frontex' Guidelines for ABC

While ABC systems are currently being rolled out at European airports, the use of these systems is not regulated by a specific law at European level yet[15]. The European Agency for the Management of

[14] Currently, 13 European countries already employ ABC systems at airports (Frontex 2013 (ABC conference report). Examples of these are EasyPass which is available at four airports in Germany; the ABC system that is used in three airports in Spain, and the Self-Service Passport Control at Schiphol Airport in the Netherlands

Operational Cooperation at the External Borders of the Member States of the European Union (Frontex), however, has developed best practices and operational guidelines for ABC systems (Frontex 2011). Although the guidelines are not mandatory, they represent an attempt to harmonise the use of ABC systems in Europe.

The Frontex document contains recommendations on the roles and tasks of personnel and the handling of exceptions. The latter outlines in which cases a traveller should be directed to a manual first line check and in which cases to a second line check. In case of 'non-cooperative behaviour at the e-gate' (e.g. moving in the wrong direction, looking the wrong way, standing in the wrong place), a traveller is to be directed to manual first line checks. In case of a failed biometric verification, however, the traveller is to be redirected to the second line check for identity verification. Where the fall-back procedure in case of a *failure to acquire* a biometric image is not stricter than the first line check by the ABC system, the fall-back procedure in case of a *failed biometric verification* is a second line check, which means that the person is considered a higher risk and will be subject to a further check. As we will see in Chapter 6, biometric technologies always produce error rates. A failed biometric verification can happen because someone is not who they claim to be, but can also be caused by a system failure. Under the Frontex guidelines, if the latter is the case, the burden of the system failure is borne by the traveller[16].

Because ABC systems have several features in common with the proposed MobilePass device, in particular in using biometric verification and (semi-)automating the border control checks, it is important for the MobilePass consortium to stay informed about the work of the Frontex ABC Working Group. The Working Group has called for a handbook for border guards that provides detailed instruction about how to deal with unwanted or unexpected situations at ABC gates. Two other FP7 projects -FastPass and ABC4EU- explicitly seek to harmonise the use of ABC gates in the EU and both have a work package dedicated to ethical, legal and social implications. MobilePass will take notice of relevant (public) deliverables on these themes in these projects.

3.3 Large-scale biometric information systems: SIS II, VIS, and Eurodac

In addition to performing document authentication and biometric verification using the e-passports of EU citizens and TCNs, the future MobilePass device may need to be able to perform background checks by accessing information systems that are external to the device. These external information systems include national databases used for border control purposes (e.g. on lost and stolen documents), and European databases.

In recent years, the European Union has created several large-scale information systems for the purposes of border control, visa, and asylum, all of which now contain biometrics: the second generation Schengen Information System (SIS II) in 2013, the Visa Information System (VIS) in 2011, and Eurodac in 2003. These databases mainly contain personal data of third country nationals: only the SIS II database also includes data on EU citizens.

3.3.1 SIS II

The second version of the Schengen Information System (SIS II) is a joint information system that is used by border guards and by police, customs, visa and judicial authorities throughout the Schengen Area. It consists of national systems (N SIS II) connected to the central part (C SIS II). SIS II holds

[16] This inherently fallible nature of the biometric matching process will be discussed more elaborately in Chapter 6.

information on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. It also contains alerts on missing persons, and information on objects and documents that may have been stolen, misappropriated or lost, such as cars or identity documents. In 2013, the SIS contained over 50 million alerts, the majority of which were on lost or stolen identity documents (39 million) (euLISA factsheet 2013). For third country nationals, a check against the SIS is systematic on entry, and non-systematic on exit. For EU citizens a SIS check is non-systematic.

In April 2013, a new version of the SIS -SIS II- was launched, which includes the possibility to use biometrics (Decision 2007/533/JHA). In particular, *fingerprints and digital facial images may be stored for the purposes of confirming identity* (RTP Impact Assessment 2013). While the SIS identification is carried out with the alphanumeric data contained in the MRZ of the travel document, **the photograph and fingerprints may be used for verification (1:1***)*. An explanatory memo by the European Commission, however, states that '[w]hen this becomes technically possible, *fingerprints may also be used to identify a third-country national* on the basis of the biometric identifier' (EC/DHA 2013-04-09). Data in SIS II is stored for a maximum of 5 or 10 years (depending on the type of alert).

3.3.2 VIS

The Visa Information System (VIS) allows Schengen States to exchange visa data. Similar to SIS II, it consists of a central part connected to the national computer systems of the visa authorities in the Member states and of consulates in non-EU countries. The VIS database contains information on visa applications by third country nationals and on visas issued, refused, annulled, revoked or extended. When a person applies for a visa, *10 fingerprints and a digital photograph are collected and stored in the VIS*. The authorities responsible for carrying out checks at external borders and within the national territories can search the VIS by using the visa sticker number together with fingerprints. Thus the live fingerprints of the visa holder are verified against the ones stored in the VIS database. **Biometric verification using fingerprints of visa holders at entry is obligatory since October 2014** (Regulation (EC) No 767/2008, art 18 (1) and (2). The biometric matching is performed by the Biometric Matching System (BMS). While in the VIS the 'raw' fingerprint images are stored, the BMS contains the biometric templates that are linked to these images. Member States are not able to access the BMS directly, but need to communicate with the BMS through the central VIS (Unisys 2008).

A search with the visa sticker and/or fingerprints results in a hit/no hit. Only in case of a hit, the competent border control authorities get access to the file to consult the visa holder's data. Where the verification (1:1 search) fails, or where there are doubts as to the identity of the visa holder, *border authorities are allowed to use fingerprints for identification (1:n search), as part of second line control*. This means that, when, for example, a person has destroyed their travel documents, the authorities can attempt to identify them by using the fingerprints. The VIS can only be accessed by competent national authorities of the Member States (i.e. visa national authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum). In addition, and on certain specified conditions, law enforcement authorities from Member States and Europol have restricted and indirect access to the VIS data[17] (Council Decision 2008/633/JHA of 23 June 2008). Data in VIS are stored for a maximum of five years.

[17] Access to VIS is granted only if it is necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences; if it is necessary in a specific case; and if there are reasonable grounds to believe that consultation of data in the VIS will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question (art 5(1)).

3.3.3 Eurodac

Eurodac is a large *database of fingerprints* of applicants for asylum and illegal immigrants found within the EU. The database helps the effective application of the Dublin convention on handling claims for asylum. Member states will take 10 fingerprints of every applicant for asylum or foreign national found illegally present on a member state's territory of at least 14 years of age. These *fingerprints will be checked against Eurodac*, to determine whether a prior asylum application has been submitted in another Member State (Regulation No 2725/2000). Eurodac works on a hit/no hit basis. In case of a hit, the competent authorities get access to the file to consult the person’s data. Data relating to asylum applications are kept for a maximum of 10 years. Data relating to foreign nationals apprehended in connection with an irregular crossing of an external border are kept for two years from the date on which the fingerprints were taken. In July 2015, a new version of the Eurodac Regulation will become applicable, which allows national police forces and Europol to access the Eurodac data under specific conditions[18], and allows the use of latent fingerprints.

3.3.4 Special rules for the use of biometrics

On a general level, the processing of personal data in the SIS II, VIS, and Eurodac is regulated by rules on personal data protection established under the Directive and Convention 108. In addition, the legislation on the processing of personal data in the context of police work *(*Council Framework Decision 2008/977/JHA, CoE Police Recommendation R (87) 15), and on the processing of personal data by *Community institutions and bodies (*Regulation (EC) 45/2001) apply*.* The Regulations governing the SIS II, VIS and Eurodac, however, also contain a number of specific provisions that complement the general data protection principles and that *explicitly regulate the use of biometrics*. It should be noted that in these information systems, the biometrics are stored as ‘raw’ data (sample images).

Data quality

According to article 22 of the SIS II Regulation, photographs and fingerprints may only be entered in the SIS II if the *quality of the data* is sufficient. A similar general obligation is laid down in Article 29 of the VIS Regulation on the ‘responsibility for the use of data’. This article states that Member States need to ensure that data are collected lawfully; transmitted lawfully to the VIS; and that the data are **accurate and up-to-date** when they are transmitted to the VIS. The new Eurodac Regulation also requires fingerprints to be of an ‘*appropriate quality’* for the purpose of comparison by means of the computerised fingerprint recognition system’. For Eurodac it is the euLISA that defines the appropriate quality and the recognition system has a built-in quality checker (Regulation (EU) No 603/2013, art 25).

Capturing of live biometrics

For VIS, Commission Decision 2009/756/EC lays down the **specifications for the capturing of live biometrics** for verification against the stored fingerprints and for identification at the external border. It states that *identification shall take place with 10 fingers flat, and verification with four fingers flat*. However, it also states that ‘Member States may decide to use one or two fingerprints flat for biometric verifications, instead of four fingerprints’. For the SIS II, however, the legislation does not contain any specifications on how biometric verification should take place.

[18] Access to Eurodac is granted only if it is necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences (art 2(1)(i)). Designated authorities need to submit a reasoned electronic request and can only do so if comparisons with national databases and Prüm databases and the VIS did not lead to the establishment of the identity of the data subject (art. 20).

Exception handling

For the VIS, a basic **exception handling procedure for the biometric verification process** at the border seems in place: The VIS Regulation states that 'For visa holders whose fingerprints cannot be used, the search [verification at entry] shall be carried out only with the number of the visa sticker (art18(3)). For the SIS II there are no rules on how exceptions should be handled.

These examples show that some basic rules are in place, but these rules still need to translated into more specific guidelines in order to be useful[19].

3.4 Future developments: the smart border package

In February 2013 the European Commission proposed two new pieces of legislation, collectively known as the 'smart border package'. The stated aims of the smart border package are 'to improve the management of the external borders of the Schengen Member States, fight against irregular immigration and provide information on overstayers, as well as to facilitate border crossings for pre-vetted frequent third country national (TCN) travellers'. The smart border package includes a proposal for an **Entry/Exit system (EES),** and a **Registered Traveller Programme (RTP)** for third country nationals. In both proposals the use of biometrics is foreseen.

A pilot with the EES and RTP will start in January 2015. The negotiations on the EES and the RTP are expected to be finalised by mid 2016, and the aim is for the systems to be operational by mid 2020 (Council of the European Union 2014).

3.4.1 Proposal for an Entry/Exit System

The Entry/Exit system (EES) will be a centralised storage system containing entry and exit data of all third country nationals (visa holders as well as those exempt from visa obligations) who are admitted to the Schengen Area for a short stay (max 90 days out of 180 days). The system is intended to tackle the problem of *overstayers*: people who have originally entered the Schengen Area with a valid short stay visa, but who do not leave when their visa expires.

While in the VIS information on visa applications is stored, it does not store entry and exit data. The Entry/Exit system would contain identity data of all TCNs admitted for a short stay as well as the place and date of entry and exit, upon each crossing of the external border of the Schengen Area (COM(2013) 95 final). The EES would also include an automated calculator that indicates the maximum authorised duration of stay in the Schengen Area of each third country national. On entry, the automated calculator informs the competent authorities and the third-country national of the authorised length of stay; on exit, it identifies third country nationals who have overstayed (COM(2013) 95 final, art. 9). The EES would thereby replace the current practice of manual stamping of passports, which, according to the proposal, is currently both 'time-consuming and difficult' (COM(2013) 95 final, p. 43), because the duration of stay often needs to be calculated from a range of different stamps with sometimes varying legibility. The EES would make data on entry and exit available in a database, instead of only in the passport where there is a risk that a stamped travel document gets replaced or lost, or is destroyed. In addition, the EES would make it easier to share data between different Member States.

[19] For example, what does 'fingerprints cannot be used' mean in practice? Does it refer to visas that do not contain fingerprints? Or does it also refer to a failure to acquire fingerprints, or biometric verification failures? There are also no rules on the consequences when the result of a biometric verification is a non-match. Is a person then considered a higher risk and treated accordingly?

The EES proposal also directs *the collection and storage of 10 fingerprints* of third country nationals of 12 years of age and older who are exempt from the visa obligation (the fingerprints of visa holders are already stored in VIS). Recording of fingerprints would commence three years after the EES has become operational. **The fingerprints would need to be collected by the border authorities at the border crossing point of entry** (art. 12)

In the proposal, competent authorities (i.e. border, visa, and immigration authorities) are allowed to search the EES with specific alphanumeric data in combination with fingerprints, both at the external border (art. 15) and within the territory of the Member State (art. 18). The purpose is to verify the identity of the third country national and/or check whether the conditions for entry to or stay on the territory of the Member States are fulfilled (art. 18). In addition, to identify a person who may not, or may no longer, fulfil the conditions for entry to, stay or, a 1:n search with the fingerprints of that person may be performed (art. 19). This may be done not just at the external border, but also within the territory of Member States. Two years from the start of the operation of the EES there will be an evaluation as to whether access to the EES should be allowed to law enforcement authorities and, remarkably, to third countries.

3.4.2 Proposal for a Registered Traveller Programme

The stated aim of the proposed Registered Traveller Programme (RTP) is to *facilitate* the border crossings of *pre-vetted, frequent third country travellers*. These travellers would participate in the programme on a voluntary basis and possibly pay an application fee. Registered travellers would then be allowed to use the same lanes (manual and ABC) as EU citizens. A registered traveller would be issued a token in the form of a machine-readable card containing only a unique identifier (i.e. application number), which is swiped on arrival and departure at the border using an automated gate. The gate would read the token and the travel document (and visa sticker number, if applicable) and the fingerprints of the travellers, which would be compared to the ones stored in the Central Repository and other databases (including VIS). If all checks are successful, the traveller is able to pass through the automated gate. In case of any issue, the traveller would be assisted by a border guard (COM(2013) 97 final).

The EC proposed to *store four fingerprints* in the central repository. It also proposed to not link the fingerprints with the alphanumeric data, but enter these data in separate sections in the Central Repository. The link between the alphanumeric data and fingerprints should be established only by the unique identifier (COM(2013) 97 final, p.13). During the border check a border guard would receive only hit/no hit information from the Central Repository. The data are to be kept for a period of maximum 5 years.

3.5 Concerns about joint information systems and the smart border package

Several advisory bodies and supervisory authorities are critical about the existing large-scale information systems and the smart border package.

3.5.1 Data protection issues

Data protection experts have expressed concern about the use of biometrics in large-scale information systems. The EDPS, in its opinion on SIS II, for example, proposed a list of common obligations or requirements that need to be respected before a biometric is introduced to an information system[20]. The Article 29 Working Party, in its opinion of the VIS, stressed the risks of storing biometrics of visa applicants in a centralised database, including the risks of misuse (WP96).

The smart border package as well has generated controversy and criticism. The Article 29 Working Party, for example, doubts whether an EES will achieve the aims of more efficient border crossings and combating overstay. Moreover, it has 'reservations about the proposals from a data protection point of view', and expressed 'serious concerns about whether the Entry Exit System meets the standards of necessity and proportionality necessary to justify its impact on the right to protection of personal data as set out in Article 8 of the EU Charter of Fundamental Rights' (WP206). The EDPS similarly concluded that the proposals 'imply an interference with the right to respect for private and family life, with possibly wide implications for the individuals concerned' (EDPS 2013, p. 25).

While in the EES and RTP proposals, the recording of biometric data is foreseen, both The Article 29 Working Party and the EDPS are critical about whether biometric data should be recorded and stored at all. The EDPS pointed out that the use of biometrics represents 'a separate interference with the right to respect for private life' and that its necessity needs to be demonstrated (EDPS 2013, p. 15). The Working Party calls for an evaluation of the system after some years of operation in order to assess whether the objectives could also be achieved without the collection of biometric data. The EDPS also has been critical about the collection and storage of all 10 fingerprints for the EES, which 'would only be needed if this pursues a different purpose, i.e. the identification of traces in a law enforcement context', and states that collecting two or four 'would in any case be sufficient for verification purposes' (EDPS 2013, p. 16). The proposed possibility to allow law enforcement authorities access to the future EES after a period of evaluation, has been criticized by the EDPS, The Article 29 Working Party and the Meijers Committee.

3.5.2 Efficiency and effectivity

While the European Commission presents the smart border package as a way to 'speed-up, facilitate and reinforce border check procedures for foreigners travelling to the EU', several parties have expressed their worries that in practice the new regulations would lead to *longer* waiting times at the border.

Where the EC already expects that the obligation to biometrically verify visa holders against the VIS will slow down the border crossing of TCNs, the proposal to also collect and store fingerprints of visa exempt third country nationals (whose fingerprints under the current legislation are *not* taken) as part of the EES, is expected to lead to additional delays (EES impact assessment 2013). The RTP is presented as compensation for the increased waiting times for TCNs due to the introduction of the VIS and the proposed future EES, but the number of TCNs that will enrol in the programme may be rather limited (Hayes and Vermeulen 2012, Meijers Committee 2013, p. 1). The EC itself estimates a maximum of 5 million new RTP applications yearly (RTP impact assessment 2013, p. 16).

The Article 29 Working Party states that in order to have an effective entry/exit system, *exit controls* need to be improved. Without these, people may suffer negative consequences from false notices of overstay. However, the Working Party expressed concern that such a working exit system could be

[20] The list, which the EDPS calls non-exhaustive, includes a targeted impact assessment, emphasis on the enrolment process as a critical step in the biometrics process, highlighting the level of accuracy for biometric identification, and the implementation of fall-back procedures to avoid the burden of failure of a biometric system falls upon the travellers (EDPS 2006/C 91/11)).

difficult to implement. Especially at land borders, it would require significant additional infrastructures and human resources (WP206).

3.5.3 Function creep

In addition to the use of biometrics as such, the access of law enforcement authorities to VIS, and in the near future also to Eurodac, was criticised by several bodies (EDPS, UNHCR, Meijers Committee). Their main concern is that these databases were established with a particular stated purpose (e.g. for Eurodac ‘facilitating the application of the Dublin II Regulation’), and that extending access to these databases to law enforcement authorities constitutes a significant step beyond the original purpose. The EDPS calls granting law enforcement agencies access to Eurodac, which is to take effect per July 20th, 2015, an example of "function creep", a gradual widening of the use of a system or database beyond its initial purpose (EDPS 2012). The UNHCR has emphasised that the proportionality, necessity and utility of granting law enforcement access to Eurodac for combating terrorism and other serious crime is not proven and that additional safeguards are needed (UNHCR 2012).

Connected to the issue of function creep are the EC’s efforts to increase interoperability between the different systems, i.e., ‘the ability of IT systems and of the business processes that they support to exchange data and to enable the sharing of information and knowledge’ (Commission of the European Communities, 2005). The EDPS warns that ‘[i]nteroperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this data via another information system’ (EDPS 2005). An example of this is when a visa authority would be able to access the SIS II via the VIS.

Current attempts by the EC to converge the different large-scale information systems take place at a managerial and technical level. The establishment of the EU Agency for large-scale IT systems (EU-LISA) for the operational management of VIS, SIS II, Eurodac and future information systems (EES, RTP) is an example of this convergence. At a technical level, SIS II and VIS already operate using the same technical system.

In addition, the *Biometric Matching System* now performs fingerprint matching services for the VIS (both for verification and identification purposes), but is intended to be used for SIS II and Eurodac as well (SEC(2009) 836). In the new Eurodac Regulation , which is to take effect from July 20th 2015, the possibility to compare a latent fingerprint with the fingerprint data stored in Eurodac by using the BMS is added (Regulation (EU) No 603/2013 article 2(1)(l)). A staff working document from the EC describes the BMS as ‘an information search engine that can match biometric data from visa applications, identity management systems and policing systems’ (SWD(2013) 47 final, p. 72). The same document states that the BMS database ‘will be able to store the fingerprints of up to 70 million people and process more than 100,000 verification and identification requests per day’ (idem). This suggests that the BMS will not just perform matching, but will also become a database in which fingerprint templates from different large-scale information systems will be *stored*.

3.6 Conclusions

The analysis of the current European legal framework for border control shows that the legal basis for biometric verification at the border is not in all cases explicit. While the recently amended Schengen Borders Code explicitly allows systematic biometric verification using fingerprints of third-country nationals against VIS at entry, the biometric verification of European citizens against the e-passport is not mentioned anywhere in the SBC. For the biometric verification of TCNs, the VIS and SBC also do not specify in detail how this process needs to be carried out, and which safeguards are in place.

The absence of a clear legal basis for biometric border checks on *EU citizens in particular* can be considered as problematic. The Schengen Borders Code does not explicitly refer to the possibility to use a person's fingerprints or digital facial images for verification. While the e-passport Regulation mentions that the biometric data *stored in the passport* may be used for verification, this Regulation does not contain specifications on the *capturing and matching of live biometrics* against the biometrics stored in e-passports. Moreover, where the use of biometrics for 'speeding up' the border passage of TCNs via ABC would be regulated by the RTP, the EC has not produced specific proposals on the use of ABC by EU citizens.

The absence of specific rules and safeguards for the use of biometrics in border control of EU citizens raises several legal and ethical questions. Does the Schengen Border Code still provide an adequate legal basis when border control is increasingly automated and the character of identity verification changes from a visual comparison performed by a border guard to a comparison of (one or two) live biometrics with the biometrics stored on a chip in the passport, performed by a technical device? More particularly, the Schengen Borders Code directs that EU citizens undergo **a minimum check** which consists of a '**rapid and straightforward verification'.** Is the use of biometrics proportional for a minimum check, especially when less intrusive means (i.e. a manual inspection) are available? Can we consider biometric verification to be as rapid and straightforward[21] as a manual verification? And, lastly, taking into account that the Schengen Borders Code regulates **manual border control** (controls carried out by a border guard), what exactly does the border guard *do* in a setting in which verification is automated (e.g. does he/she fully rely on the results produced by the technologies?

4. Summary of legal requirements and implications for MobilePass

In the base line scenario, the MobilePass device would be used at the external European land borders for document authentication, background checks, and traveller biometric verification on the basis of fingerprints and facial images for both EU citizens and Third Country Nationals. The main legal aspects are:

1. The **legal basis** for (biometric) checks at the border is not straightforward. The relevant rules and regulations are dispersed, subject to (imminent) change, and different for different categories of travellers

2. There is an overall distinction between **EU citizens** and **third country nationals** (TCNs) with regard to the type of biometric checks that are allowed/mandatory.

3. Biometric data are to be considered as **high risk with regard to privacy invasion (see 4.1)**, and in all cases **subject to the strictest data protection regulations (see 4.2)**.

4. Depending on the extent to which the Mobile Pass device is to accommodate **future developments**, additional requirements need to be taken into account (see 4.3).

[21] In Chapter 6 we discuss how the idea that biometric technologies would produce 'straightforward verification' can be challenged when we understand a biometric matching process as a chain of translations which produces probabilistic results.

4.1.Mobile biometric border control and the right to privacy

The European Court of Human Rights (ECtHR) has ruled in several cases that the processing of biometric data is an interference with the right to privacy (art 8 ECHR and art 7 EUCFR). The processing of biometric data by the MobilePass device in the foreseen scenarios might also be considered an interference with the right to privacy[22]. This would mean that three questions need to be asked:

1. Is the aim of (improving) border control of persons crossing the external borders of the Member States of the European Union a legitimate aim?

2. Is the interference in accordance with law? Do European and national laws governing border checks on persons provide for the measure employed?

3. Is the measure employed necessary in a democratic society. In other words, can the same (legitimate) aim be achieved with less invasive means?

On a general level, the aims to secure, facilitate, and speed up border control of persons crossing the external borders of the Member States of the European Union can be considered a legitimate aim. The crucial questions are if the use of biometrics to achieve this aim is *in accordance with the law* and can be considered *necessary*.

As we have seen above, there are serious gaps in the current legal framework for biometric border checks on EU citizens in particular. **It is questionable if the current legislation at European level is sufficiently clear and precise in terms of the conditions for storing, using and deleting biometric data to allow for the processing of biometric data in the minimum check for EU citizens**. This would mean that specific laws at national level are required.

In assessing the proportionality of the use of biometrics in border control of *EU citizens in particular*, the balance between the benefits of using biometrics (higher level of security and facilitating/speeding up border passage) and the interference with the private lives of EU citizens is crucial. In other words, is the measure (i.e. the use of biometric verification in the first and second line minimum check) necessary in a democratic society, in particular when less intrusive means are available in the form of visual inspection? Here an important question is if the necessity to make border checks on EU citizens more secure can be proven, and whether biometric verification would really decrease the time EU citizens spend at the border check point compared to the present manual verification. **If the benefits of security and speed do not outweigh the loss of privacy, the use of a mobile biometric device as part of the minimum check could easily be considered disproportionate.**

4.2 Mobile biometric border control and the right to data protection

Regardless of whether or not the processing of biometric data with the MobilePass device can be considered an interference with the right to privacy, the processing of biometric data is a form of personal data processing, and hence the Data Protection Directive automatically applies.

Even when under the Data Protection Directive, biometric data are not considered a ‘special category of data’ (of which the processing is in principle prohibited), they must be considered as presenting risks to the rights and freedoms of data subjects. **Biometric data processing with the help of the**

[22] A judge would need to decide on this

MobilePass device therefore must comply with the strictest data protection rules (as laid down in the Data Protection Directive, and, in in the future, in the Data Protection Regulation)

The main data protection principles in the Directive are the legitimate processing of personal data, and data quality principles (fair and lawful processing, purpose limitation, proportionality, data minimisation, data accuracy, data retention). The Directive also imposes obligations upon data controllers, and provides rights for data subjects. Below we outline the implications this has for the processing practices enabled by the MobilePass device. This preliminary analysis also forms the basis for deliverable 2.2, in which we will develop guidelines and recommendations for the design and use of the MobilePass device.

4.2.1 Legitimacy

The processing of biometric data with the MobilePass device needs to have a legitimate ground. For EU citizens, there is currently no law making biometric verification of EU citizens at the external border mandatory. It is therefore questionable whether the processing can be done on the grounds that it is necessary 'for compliance with a legal obligation to which the controller is subject done (Art. 7c), 'for the performance of a task carried out in the public interest' (Art. 7e), or 'for the purposes of the legitimate interests pursued by the controller' (Art. 7f). This means that biometric verification of EU travellers **must be presented to the travellers as an option, and be based on the informed consent of the traveller**. If biometric verification of EU citizens would take place without their (explicit) informed consent, this could be considered a breach of data protection principle of legitimacy. Because under the new Data Protection Regulation consent needs to be *explicit*, and the controller has the burden of proving that the data subject has given the consent, **the MobilePass device configuration might need to be able to *documen*t the travellers' consent.**

4.2.2 Data quality principles

For the processing of biometric data with the MobilePass **a specified, explicit and legitimate purpose needs to be defined, and data should not be further processed in a way incompatible with those purposes**. If, for example, the data captured by the MobilePass video camera is processed for the purpose of verification of the captured image with the one stored in the passport (or in a database), then using the video images for the general surveillance of travellers would constitute a breach of the purpose limitation principle.

Data must be 'adequate, relevant and not excessive in relation to the purpose for which they are processed' (proportionality and data minimisation). In 2.1.3 we showed how a proportionality test, for the MobilePass biometric system would ask whether the system is *necessary* to meet the *identified need,* if it is *effective* in meeting that need, if the *loss of privacy is proportional to any anticipated benefit* , and if the same goals could be achieved *with less intrusive means.* There are clearly **challenges in demonstrating the proportionality of the MobilePass device, in particular when the device is used as part of the minimum check.** This makes it important for MobilePass to demonstrate that only the necessary data is processed, and not more. For example, is it necessary to **process both fingerprints and facial images** as part of the minimum check? Another issue is the number of fingerprints that are taken. **For verification of fingerprints against the e-passport, only two fingerprints would be needed** (as e-passports only contain two fingerprints).

Data must be 'accurate and, where necessary, kept up to date'. This is also a challenging requirement, because the MobilePass device is used in diverse ambient conditions (outdoor, inside vehicles) and makes use of new capturing technologies (touchless fingerprint and video-based facial images). The MobilePass device, **must be able to process data accurately under diverse ambient conditions**: the fingerprints and facial images obtained in outdoor conditions or inside vehicles need to be of sufficient quality, and the matching algorithms need to be able to verify samples obtained under different environmental conditions against reference images taken in controlled environments with low error rates. Also, the **processing of fingerprints and facial images produced by the specific capturing technologies must be accurate**: the fingerprints and facial images captured with the new technologies need to be of sufficient quality, and the matching algorithms need to be able to verify these samples against references images produced by conventional technologies (touch-based fingerprint/facial photograph) with low error rates.

Data also must 'not be stored longer than necessary'. While the aim is that the MobilePass device does not store data, **there are scenarios in which temporary storage may be necessary**. For example, when border checks are conducted in a train departing from a station in a neigbouring non-EU country, it may be necessary to store data until arrival at the first station on the territory of the Member State.

4.2.3 Data controllers' responsibilities

Because biometric data present risks to the rights and freedoms of data subjects, **the processing of biometric data by the MobilePass device must be highly secure**. This is even more important when it is *biometric samples* (instead of templates that are transferred and possibly temporarily stored on the device or a server.

4.3 Accommodating future developments

In the smart border package proposals are developed concerning the development of an Entry-Exit system (EES), and a Registered Traveller Programme (RTP) for TCNs. Any implementation of these proposals has implications for the functioning, and hence, for the requirements of a mobile border checking device.

In particular, to accommodate the device's possible role in the EES, **it needs to perform as an enrollment device:** it should be able to capture the 10 required fingerprints on entry of visa-exempt TCNs, and upload these to the EES. This function requires it to conform to an additional set of technical and quality standards.

In addition, if the device is to accommodate the planned RTP, **it needs to be able to execute verifications on the basis of a yet another token-based numeric identifier as well as fingerprints stored in the RTP Registry.** This requires the device to conform to the technical and quality standards involved in that system.

Finally, the VIS Regulation already allows the use of fingerprints for identification, and there are proposals to allow identification using fingerprints against SIS II and the EES. If the device is to have the **capacity to perform identification**, it needs to conform to an additional set of technical and quality standards

Part II

Social and ethical aspects of mobile biometric border control

The second part of this report discusses the social and ethical aspects of mobile biometric border control. In discussing social aspects, the focus is on how technology brings along changes and effects in social relations (e.g. power relations), identities, or the treatment of (categories of) people. Such changes may have ethical impact when they touch upon values, principles, and norms, such as equal treatment, respect for persons, justice, in- and exclusion, privileging, and various types of freedom

Before presenting the analysis of social and ethical aspects, we first briefly explain our conceptual approach in Chapter 5. In contrast to the common view of technology as inherently neutral (with social and ethical implications conceived as *consequences of particular uses and applications of the technology*), we base our analysis on theories from Science and Technology Studies (STS). We use the concept of *affordances* to analyse how technologies, as part of *particular socio-material configurations*, may bring along certain social effects and ethical issues.

In Chapter 6, we 'unblackbox' the process of biometric recognition to show how biometric systems in processing biometric data always afford the occurrence of errors and uncertainty. This has important social and ethical implications, even more so because it appears that errors and uncertainties are distributed unevenly among different users of biometric systems.

Chapter 7 focuses on how biometric systems afford (new) information processing practices such as automated processing, categorisation, and the transfer, sharing and linking of data. These practices however also carry specific risks such as covert surveillance, identity theft, misuse or unauthorised use of data, and differential treatment of people.

Finally, Chapter 8 discusses how handheld biometric devices afford the 'portability' of the biometric border. This transforms the managing and controlling of the movement of people across borders, and these transformations bring along various social and ethical issues.

In the conclusion of each part we describe challenges for designers, implementers, operators. These conclusions form the basis for the guidelines that will be developed in Deliverable 2.2.

5. Conceptual approach

5.1 Introduction

There is a widespread view concerning technology in general that it is inherently neutral, and that social and ethical implications only emerge as the *consequences of particular uses and applications of the technology*. This view includes the idea that technical aspects are essentially separate from ethical and social aspects.

Such a view, however, implies that any analysis of the social and ethical aspects only makes sense *post hoc*, and that any potentially negative ethical and social implications are logically dealt with afterwards only, usually by regulating use and application of the technology in question.

In contrast, we proceed from an alternative view that sees technology as a human practice, best analysed as a heterogeneous socio-material configuration. This view is based on several decennia of research on the mutual shaping of technology and society usually referred to as 'science and technology studies or STS. From this body of academic literature, in particular from one of its main theoretical approaches called Actor Network Theory, we take a set of key concepts and insights that will enable us to analyse the social, ethical and legal aspects of the MobilePass project in a way that is proactive rather than reactive. Moreover, it allows us to highlight potential issues in a way that is intended as constructive rather than merely critical.

5.2 'Technology' and 'society' as mutually constitutive

Perhaps the most central insight that has emerged within STS is that the development of technological systems does not follow a path of a purely technical rationality that exists separate from society and its value systems. Instead, all kinds of considerations and contingent factors play a role in every stage of the development of technologies. These considerations and factors may be of a technical nature, but may equally be economic, cultural, organisational, social, legal, ethical in kind. They may also include highly contingent, local, even serendipitous or psychological factors. Moreover, even if at a certain point the technology can be said to have stabilized to a certain extent, after which it becomes 'implemented', 'applied' and 'used', generally it does not stop evolving or further taking shape: users may adapt it, change settings and functions, find new uses, or give different meanings.

In addition, technologies require and assume many things to be there to actually 'work' that are not usually considered part of the artefact as such, but that need to be taken into account to fully assess social and ethical implications. Such things may include an elaborate pre-existing operational technical infrastructure, but also a particular (re-)organisation of work, a spatial-material organisation of the setting, and, crucially, a specific set of users with prescribed behaviors, and a set of assumed characteristics, goals, beliefs, and interests. It is in these presuppositions and assumptions that many of the social and ethical implications of a particular, device usually lie. Therefore it is this composite object we refer to as the socio-material configuration of a technology that forms the object of the analysis presented in this Deliverable.

This approach has similarities with, but differs from an approach that analyses technology in its 'context of use', in that the latter presupposes the technology to exist as finished and stable black box, with inherent characteristics prior to this 'context'. Conversely, this framing presupposes a stable context to pre-exist independent of the technology. We, on the other hand, need an approach that allows us to analyse both technology and context as co-constituting each other: it is not only the use context - both as a set of ideas about future use during the design phase, and as the practical setting where actual implementation and take-up takes place - that is actively involved in shaping the finalised technology. It is also the case that, conversely, the technology usually (re-)shapes its own context of use in many intended and unintended, minor and major ways. Moreover, it is to significant extent in this mutual constituting process that social and ethical implications usually are to be found.

To be sure, this mutual shaping of 'technology' and 'context' plays out on more than one level. It can be seen to occur on the 'micro level' of individual border guards' work at concrete border crossing points, dealing with individual travellers. Here, 'requirements' from the setting and routines into which the technical device is to fit, are collected from these 'end-users', and translated into the specifications that guide its design. On the other hand, however, border check routines, and the spatial-material as well as the social organisation of these, will change and adapt in more and less subtle ways to allow the device to 'fit in' and function properly.

But a similar process occurs on a more macro level of European and national politics and policy. Here, technological developments involving new identification and verification modalities, monitoring and registration systems, as well as assumptions about their availability and functionality, more or less implicitly play a role in resetting policy goals and agendas. In particular in the areas of border and migration management, mobility and security policy, several new programmes and agendas have been developed in recent years that could only be formulated as such with the new technological capabilities in mind. For example, what counts as secure and expedient border management is today increasingly defined in terms of efficient, secure, preferably automated, identity and document verification; asylum and visa policies today presuppose the availability of operational databases that are accessible by border officials at Europe's external border crossing points. Thus, in this sense technology can be seen to play a role in producing new or changed political agendas and policies, as opposed to being mere neutral instruments, developed to implement certain political programmes.

In this Deliverable, we focus on the way 'technology', in this case a mobile, portable border check device, involving multiple (biometric) verification modalities, is both shaped by, and itself could play a part in reshaping, border check practices at land borders. To capture this dual, co-constitutive process, we consider the MobilePass device as a *socio-material configuration*, enabling and constraining, or *affording* particular ways of doing border checks.

5.3 Key concepts

To analyse this complex object, we make use of a few key concepts and methods. [*tbd*]

6. Biometric recognition as a chain of translations

6.1 Introduction

One of the reasons for the attractiveness of biometrics is that the body is thought to provide an objective and verifiable source of truth about a person's identity (Martin and Whitley 2013). An often heard argument of biometrics advocates is that "the body does not lie" and biometric technologies are believed to give access to these 'truths' in a direct way. The claim that biometrics reveal 'the truth' about someone's identity, however, can easily be dismantled. First, biometric systems verify a *claimed* identity: biometrics only match a biometric with a particular file describing an identity and whether this identity is correct or false (e.g. based on a falsified birth certificate) is another question (Ashbourn 2014). Second, the result of the biometric matching is not conclusive in confirming or denying an identity (idem), but only indicates the degree of similarity between biometric probe and one (or more) template(s). Third, there is no *direct* link between body and identity: **The process of biometric recognition is a chain of translations of body into information** –from body part, to image, to feature set, to a match/non match output. Each step in this chain of translation introduces a certain extent of contingency, and, hence, room for deviation and error (Van der Ploeg & Sprenkels 2011).

In this chapter we investigate this chain of translation by focusing on how the body is translated into pieces of information and processed in order to generate a biometric recognition result. We discuss how biometric recognition is probabilistic and how as a result biometric systems *afford the occurrence of errors and uncertainty.* Next, we explain how biometric systems *afford a particular distribution of errors* among the individuals and groups using a biometric system. We relate this to the problematic premises of biometric science, and the often implicit normative assumptions about bodies and users that get inscribed into biometric technologies (Van der Ploeg 2012). By using examples from the biometrics literature , we also shortly discuss how the *attribution* of errors to either technologies or users, shapes the spaces where solutions and adaptations are expected to be found and applied.

6.2 Biometrics, errors, and uncertainty

Biometric systems establish a link between a body and a stored template, but in doing so afford the occurrence of errors and uncertainty. A few years ago, the United States National Research Council in a report emphasised that '[n]o biometric technology is infallible; all are probabilistic and bring uncertainty to the association of an individual with a biometric reference […]' (Pato and Millet 2010, p. 52). The components of a biometric system –the sensors that are used, the feature extraction algorithms and matching algorithms- all contribute to the production of errors in the process of translation.

First, the translation of physical characteristic of a person into digital representation by the sensor always involves the loss of some information and the introduction of what the biometrics literature refers to as 'noise'. In the next step, the biometric sample is transformed into a biometric template by feature-extraction algorithms, which again is a translation in which some information is added and other information is lost. Next, a matching algorithm matches the biometric probe with a stored biometric template. Here the process is a.o. influenced by what is referred to as the 'quality' of the algorithm and the biometric reference template, and in the case of 1:n matching also by the size of the reference database[23]. The result of biometric recognition is therefore not a binary yes/no answer to the question whether the two compared feature sets (sample and template) match, but a comparison score, which is a *probabilistic* result. A comparison score of 80% for example means that the algorithm estimates 80% similarity between biometric probe and biometric reference. A perfect comparison score of 100% is virtually impossible, because even when the same biometric characteristic of the same person is measured, each new sample will differ a little from the previous one[24].

The probabilistic nature of biometric recognition brings in errors and uncertainty. The outcome of the process of translation of physical characteristic into biometric recognition result is never completely 'accurate'. This also implies that there is always a chance –even if it is just a very small one- that the outcome of the biometric recognition process is incorrect (see *false rejects*, *false accepts*). In a biometric system what counts as a 'match' are the comparison scores that exceed a certain chosen *threshold*. Changing the threshold therefore means changing what counts as a match. What is considered an 'appropriate' threshold depends for example on the aim of the system and on its operational context. When biometrics are used for accessing a theme park (as in Disney World), a higher level of false accepts is more acceptable than in a high security context such as border control, where the number of false accepts should be kept as low as possible. Also, a system administrator can adjust the threshold of a system when operational circumstances require this. For example, to increase convenience, the threshold of an iris recognition scheme at an airport can be lowered (so that less false rejects are produced).

6.2.1 Social and ethical aspects of errors and uncertainty

The affordance of biometric systems to produce errors and uncertainty brings along several social and ethical issues.

First, while the production of errors will always affect a part of the users of a biometric system, this will be particularly problematic when biometric technologies are used in large-scale applications. For example, an error rate of 0,1 % seems almost perfect. Yet, when biometric technologies are used in areas such as border control, with millions of users, large numbers of people will be affected every day.

A second important issue is the amount of trust that is put in technology. When too much trust or authority is put in a technology that inevitably produces errors and uncertainty, this may have negative consequences for the people using the biometric system. For example, when during a biometric verification process a person's live biometric image does not match with the image stored in the e-passport, this might be caused by the fact that the person is carrying a false passport, but it might also be a false reject. When a non-match is automatically assumed to be a false identity claim by an imposter, this may lead to situations in which the burden is on the person to prove that she is the legitimate holder of the passport, and to a violation of the presumption of innocence.

On the other hand, when many false non-matches take place, this may consume a lot of resources and time from biometric system operators. As a result, operators may become inclined to treat non-matches as errors, and this would make the border crossing process less secure.

[23] False-match errors generally increase with the number of required comparisons in a large-scale identification system (Pato and Millet 2010).

[24] These variances are for example due to different sensing conditions (e.g. the position of the camera), changes in a person's biometric characteristics (e.g. due to ageing), differences in the way a person interacts with the system (e.g. their pose), and different environmental conditions during measurement (e.g. temperature, humidity).

The setting of the threshold also brings along social and ethical issues. The setting of the threshold determines the 'acceptable' number of false non-matches and false matches, and this has real consequences for the people using the biometric system. For example, when the threshold is set at a high level, but the quality of either the live images, or references images[25], is low, this will lead to a high number of false non-matches. Because the threshold can be adjusted, this also means that the 'security' a biometric system produces is variable. Moreover, while biometrics are often claimed to enhance both the speed and security of border crossing, in operational contexts the setting of the threshold of a biometric system may be a trade-off between security (high threshold) and convenience and/or speed (low threshold)[26].

Another important aspect of the uncertainty and errors that biometric systems afford is that errors are *not randomly distributed*. In the remainder of this chapter we explore how and why some individuals and groups have a greater chance to experience biometric errors than others, and the social and ethical implications this has.

6.3 Biometrics and human differences

Biometrics can be understood as producing a 'readable body': it transforms the body's surfaces and characteristics into digital codes and ciphers to be 'read' by a machine (Van der Ploeg 2005). However, not all bodies appear equally 'readable'. Some individuals or groups are particularly hard to enrol in biometric systems, for example because they miss a particular biometric characteristic or because the technology fails to measure the characteristic. It can therefore also be argued that biometrics is producing 'differentially readable bodies' (see also Murray 2007 for the plural use of the term). In order to understand why some bodies become less 'readable' than others in the practice of biometric processing, we first need to uncover the underlying assumptions that biometric systems 'make' about bodies.

6.3.1 The problematic premises of biometric recognition

The biometrics literature describes the science of biometric recognition as being based on the two premises of *uniqueness (also: distinctiveness)* and *permanence* (Jain et al 2011). The first premise entails that 'any two persons in the world can be differentiated based on the given identifier', while the second premise is that biometric identifiers do not change over the lifetime of a person (idem, p. 13). In addition, underlying the idea of biometric recognition is the assumption of *universality,* which entails that everybody possesses the biometrics trait, and that this trait is *measurable (also: collectable)*. Hence, biometric characteristics are assumed to be unique, permanent, universal and measureable.

In practice, these premises are problematic in several ways. In the biometrics literature, it is acknowledged that the first two premises of uniqueness and permanence are not based on scientific evidence (Jain et al 2011). The premise of uniqueness, for example, is challenged by genetically related individuals, who may have faces that are almost the same, which makes facial image recognition challenging. Also, bodily features change over time: fingerprints get worn, the shape of faces change, but also weight loss or gain, plastic surgery, or scars and injuries challenge the premise

[25] The EC for example has expressed its concern over the 'insufficient fingerprint quality' of fingerprints stored in the VIS (COM(2014) 292 final).

[26] When biometrics are used in border control, for example, 'security'can be enhanced by increasing the threshold (less travellers will be falsely accepted), but this will be at the expense of falsely rejecting more people, which may lead to inconvenience for users and border guards (e.g. delays and more unnecessary second line checks).

of permanence. The changing of the biometric characteristics of a person over time –- means that the enrolled template over the years becomes a less accurate representation of the user's biometric characteristics. The biometrics literature refers to this problem as 'template ageing'. Since many European biometric passports are now valid for 10 years, we can expect the problem of template ageing to become more prominent in the near future. One group that might experience template ageing to a larger degree are (young) children, as their physical characteristics may change a lot in only a few years of time. The fact that some countries provide children as young as 12 (Austria) and 13 (Poland) years old with passports that are valid for 10 years may therefore be a reason for concern. Next, while everybody is assumed to possess the human bodily features that are used in biometrics (universality), it is clear that for example not all people are born with 10 digits, and that during their life people may lose body parts due to accidents or diseases.

6.3.2 Normative assumptions: 'normal' and 'available' users

Another important general issue that makes biometric recognition problematic, is the fact that what is referred to as 'biometrics' are not the unique physical characteristics in themselves, but *digital measurements* of these. First, these measurements introduce variations in samples of the biometric characteristic of a person obtained over a period of time, because factors such as lighting, pose, and humidity vary with each scan or image (Jain et al 2011, p. 13, see also our description of how biometric systems work). Second, the specific settings of the (components of a) biometric system (e.g. the sensor device, the algorithms) define whether a biometric trait is measurable at all. Some eye colours, fingerprints or faces may fall outside the boundaries of what a sensor device is able to capture, or what an algorithm can transform. In other words, some people's bodily characteristics appear particularly hard to acquire, digitise, or compare. The differential readability of bodies is partly the result of particular normative assumptions about bodies and users that are embedded in biometric systems.

Underlying biometric recognition is an assumption that everybody has unique bodily characteristics, but at the same time there is an assumption that everyone is similar in the sense that every human person is assumed to have a clearly audible voice, a set of ten fingerprints, two irises, and a recognizable face, and so on. With respect to the human bodily features used in biometrics, this means that there is an assumption of *normality* that is defined as a range of variations that constitute 'the normal'. Such notions of normality are built into the equipment: hand scanners have particular shapes, with designated places to put the fingers; fingerprint systems are designed for the registration and comparison of a particular number of fingerprints, cameras to scan faces are directed at a specific height, and the accompanying face recognition software often works best for a particular shade range of skin colour, and so on (Van der Ploeg 2012). While biometric science takes the 'distinctiveness' of physical traits as a premise, it may hence be more useful to see distinctiveness as an *outcome* of the process of digital measurement.

In addition to a 'normal' body, biometric systems presuppose a particular *availability* of the user and their body (Van der Ploeg 2012). The acquisition of images requires bodies to be positioned in particular ways, for example to place fingerprints on a scanner, stand still for some time, look straight into a camera. This might be more difficult for children, people with certain disabilities or diseases, and elderly people. In some contexts gender plays a role: A study on India's national biometric ID scheme reports that for the female urban poor in India, the process of enrolling their iris biometrics was more demanding and uncomfortable than it was for males:

> 'Many women could not get the photograph and their iris scan right. Trained to lower their gazes or veil their faces in an act of modesty, they were uncomfortable when staring straight into the light of a camera. Their bodies resisted the humiliating intrusion by blinking and

> producing streams of tears. A box of tissues and the authoritarian hands of enrollers—which arrested heads and pulled the tissues below and above the eyes to discipline nervous eyelids—helped the process roll on' (Rao & Greenleaf 2013, p. 294).

Embedded in biometric systems is hence a specific idea of *normality* – the range of variation of human bodily features a system accepts, and a particular scripting of the ways in which users need to be *available* for biometric processing (Van der Ploeg 2012).

6.4 How 'normal' and 'available' users are constructed in the design phase

In line with Introna's disclosive ethics approach, we can attempt to identify particular moments in the design of biometric systems at which practical choices and technical decisions are made that may at a later stage cause problems or disadvantages for its users.

6.4.1 Capturing technologies

Capturing technologies, such as cameras for taking facial images or fingerprint scanners, work with particular built-in norms about the bodies and behaviour of their users. Yet, it is difficult to pinpoint exactly how and when capturing technologies come to 'favour' particular bodies and users. According to cultural theorist Joseph Pugliese (2007, p. 107), a number of biometric capturing technologies are '*infrastructurally calibrated to whiteness*'[original emphasis]. He argues that 'whiteness is configured as the universal gauge that determines the technical settings and parameters for the visual imaging and capture of a subject.' An example would be that when the camera settings for lighting are optimised for white-skinned subjects, this makes the acquisition of the features of non-white subjects more difficult. Pugliese's argument is not that infrastructural whiteness is the result of racist thinking in the design phase, but rather that it is often *unintentional* and *hidden*. We can add to this that it is not just the fact that infrastructures are calibrated to *whiteness* that is problematic, because a calibration to 'brownness' would be similarly problematic. In addition, what a scanner is able to capture is also dependent on other 'calibrations', such as the height of a camera, the number of fingerprints it requires etc. (something we referred to above as the *availability* of users). **What is problematic is the *selective* working of the capturing technology to measure bodily behaviour and characteristics, and -more specifically-, to measure 'distinctiveness'.**

6.4.2 Algorithms

In the development stage of biometric technologies, algorithms are exposed to a set of images in order to train them to detect and extract features. In other words, algorithms learn to detect and extract features through *experience.* It is therefore somewhat surprising that there is only little research into how exactly the composition of training sets relates to algorithm performance. An exception to this is a recent study on the performance of facial algorithms developed in different regions. The study examined the performance of facial recognition algorithms developed in the West and in East Asia to match identities in pairs of Caucasian and East Asian faces (a verification task) (Phillips et al 2011). It was hypothesised that the place where the algorithms were developed (Western countries vs East Asian countries) would affect their accuracy in verifying faces from different populations (Western vs East Asian). The study concluded that the 'Western algorithm' was better at verifying Caucasian faces and that the 'East Asian algorithm' performed better on East Asian face pairs.

Phillips et al have indications that the Western algorithm was trained with the FRGC (Face Recognition Grand Challenge) dataset, which is composed of a strong majority of Caucasian faces

(70%) and a minority of East Asian faces (22%). Similarly, they assume that the East Asian algorithm was trained with a database containing a majority of East Asian faces. The study concludes that 'demographic origin of face recognition algorithms and the demographic composition of a test population interact to affect the accuracy of the algorithms' (Phillips et al 2011, p. 7). The findings also indicate that there is a need to conduct similar studies on the relation between the composition of training sets and algorithm performance on different genders and ages. **In general, this points to the importance of the composition of training sets being representative of the population that will become the users of a particular biometric system. If this is not the case, the algorithms may be trained to perform well on a too small range of actual bodily differences**.

6.4.3 Sociomaterial configuration

Another moment in the development phase in which choices are made that may influence the performance of the biometric system is the phase of scenario testing. In scenario testing, the performance of a biometric system is tested under conditions that are similar to those of the future 'real-world' operation of the system. Ideally, this includes testing under different ambient conditions (lighting, humidity, temperature, motion etc) and testing with a group of volunteers that is representative of the future user population, not only regarding bodily differences, but also in terms of user behaviour. For pragmatic reasons, however, developers may choose to recruit volunteers under university students, lab workers, or company employees. However, such groups are often not representative of the future users in terms of age, gender, and ethnicity, and may also be more knowledgeable than the average user.

6.5 The attribution of biometric errors

We have discussed how biometric systems afford a particular distribution of errors and uncertainty. In this section we give a few example of how this affordance is problematized in the biometrics literature. We discuss in what terms the unequal distribution is explained, and whether and how human and bodily differences come up in these explanations. […]

6.5.1 The biometric menagerie: a taxonomy of user groups

In biometrics science the term 'biometric menagerie' refers to the fact that in biometric systems some users are consistently 'performing poorly as they cause a disproportionate number of verification errors' (Yager & Dunstone 2010, P. 220). Historically, a menagerie is collection of wild or exotic animals kept for exhibition, but the term can also generally refer to a varied mixture (Webster dictionary). In the literature on the biometric menagerie, four animal metaphors are used to describe different user groups of biometric systems: sheep, goats, lambs, and wolves. These (rather unexotic) animals are chosen because they represent a particular 'behaviour' in a biometric system. Yager and Dunstone explain how sheep and goats refer to users who are matched against themselves, while lambs and wolves refer to users who are matched against others. When matched against themselves, sheep 'tend to match well', while '[g]oats are subjects who are difficult to match'. When matched against others, '[l]ambs are vulnerable to impersonation', while '[w]olves are exceptionally successful at impersonation and prey upon lambs' (Yager & Dunstone 2010, p. 220).

With the concept of the biometric menagerie, the biometrics literature acknowledges that FRR and FAR for a biometric deployment 'are dependent on the specific individuals utilizing that system' (Howard and Etter 2014, p. 627). In this way, failure to read a body, or failure to recognise a user is implicitly attributed to the users and not to the biometric system: it is the users who *perform poorly* and *cause errors* (see also Murray 2007). Also, in the literature on the biometric menagerie, user groups are ‘constructed’ through their ‘behaviour in a biometric system’, and the question whether ‘sheep’ are for example more often people with a specific ethnic background, does not come up.

6.5.2 Ascribing errors to ‘intrinsic’ characteristics of users

There are a number of studies in the biometrics literature that investigate whether different matching scores *are related to human differences* such as gender, age, and ethnicity. In a recent publication, two biometric experts report on their research into how ‘certain intrinsic properties of the subject’ (in their case ethnicity, gender and eye colour) influence the distribution of errors in iris recognition and conclude that ‘[p]articularly, Asian and African American individuals with brown eyes have a distinct propensity for being incorrectly not identified by iris recognition systems’ (Howard & Etter 2014, p. 631). Another study on the performance of facial recognition algorithms concludes that:

> ‘First, as in previous studies, younger adults are harder to recognize than older adults. This finding is one of the few to appear consistent in all studies, and it is rapidly gaining stature as an accepted fact. The second finding is that males appear easier to recognize than females. […]. Finally, as in past studies, East Asians are showing up as more easily recognized than are Caucasians in datasets with a majority of Caucasian subjects.’ (Beveridge et al 2009, p. 762).

Although the studies in these examples go beyond the descriptive concept of the biometric menagerie and seek to understand how biometric errors relate to gender, age and ethnicity, they still attribute failure and errors to the users. By stating that younger adults *are* harder to recognise, or that Asian individuals with brown eyes *have* a distinct propensity for experiencing errors, they make it a characteristic of these persons, rather than presenting it as the particular way in which the *technology* works.

Yet, this does not mean that the biometrics literature simply attributes failures and errors to the users. Jain et al (2011, p. 22) for example indicate that fingerprint biometric systems ‘may fail to extract minutiae features in images obtained from a subset of people who may have cuts or bruises on their fingers, or whose fingerprints are worn-out due to age or hard manual labor’. Jain here has a different way of approaching failed verification: the failure is attributed to the biometric system, instead of to the users. The biometrics literature also acknowledges that failures occur when people ‘cannot interact correctly with the biometric user interface’ (Jain et al 2011, p. 22)

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

6.6 Social and ethical aspects of the unequal distribution of errors

While it is sometimes argued that the differences in the performance of biometric systems on different users are not very large, an unequal distribution of errors rates can have major social and ethical implications. When the risk of biometric errors are disproportionally borne by particular individuals or groups, this goes against the principle of fairness. This becomes even more problematic when a particular distribution of errors is related to and interacts with differences in race, ethnicity, age, or gender. A particular distribution of biometric errors may then have political effects such as exclusion of particular groups and uneven surveillance, and affect norms and values such as equal opportunity, equal treatment, and non-discrimination.

The example of the Indian Unique ID programme shows how an unequal distribution of biometric errors can potentially lead to exclusion of particular groups. This program was set up with the goal of providing a unique identification number to every resident to access government services and includes two biometric identifiers: fingerprints and iris. Several studies however suggest that marginalised people such as the poor and elderly people have more difficulty to enrol in the scheme, due to worn fingerprints, missing fingers, and eye diseases. Hence, it is precisely the most vulnerable people who are potentially excluded from societal goods provided through the UID (e.g. welfare schemes, pension payment). Whether or not failure to enrol also results in actual exclusion, however, depends on the fall-back option of the system, or in other words, on the handling of 'biometric exceptions'. Although official reports mention that 0% of people were rejected an UID number due to biometric failure (refer to performance report), there are social scientific studies that indicate that people who fail to enrol in the UID are subjected to lengthy bureaucratic procedures (Thomas 2014) or that these procedures are simply not in place (Rao & Greenleaf 2013).

Biometric errors may also result in self-exclusion, in which those people who have more problems interacting with the system start avoiding to use it (Rebera & Guihen 2012). For example, images captured from older persons are likely to be of lower quality than those taken from younger persons (see Rebera & Guihen 2012). This means that elderly persons may experience relatively more errors such as failure to enrol or false rejection when interacting with the system. Rebera and Guihen give the example of a border control context, in which the system fails to identify an elderly person. Even though there might be a fall back option in place, this person may still feel embarrassed or humiliated. This 'encourages a form of self-exclusion whereby older people avoid putting themselves in potentially humiliating positions, and thereby restrict their access to those goods that are often mainly available via biometric identification (e.g. air travel)' (Rebera & Guihen 2012, p. 413). The fact that the European population is ageing means that the relative size of the group that experiences these problems in the context of European biometric border control can be expected to increase (idem).

In surveillance contexts, other potential effects arise. Introna and Wood (2004) discuss the use of biometric technologies for facial recognition in CCTV. They argue that in a use scenario in which the goal is to identify faces of known criminals in the crowd, the fact that particular algorithms more easily identify particular groups of people (e.g. older people, people of a particular ethnical background) may mean that this bias group will have a greater probability of being (falsely) recognised and hence may experience greater scrutiny.

These examples also show that making general claims about the social and ethical effects of distributed errors in biometric systems is not fruitful. Such effects are not the *direct* result of a particular distribution of errors, but also depend on the particular socio-material configurations of the biometric system and the larger social orderings it (re)produces. For example, if in a verification scenario, someone experiences failure to enrol or is (falsely) rejected, the availability and organisation of the fall-back option and the procedure to deal with failed verification (which are part of the configuration of the technology) is crucial in whether or not this results in discomfort, or even exclusion.

6.7 Conclusion

It is important that those who design, implement (e.g. public authorities) and operate biometric system (e.g. border guards) **acknowledge biometric processing as a process of translation and take into account that biometric technologies afford errors and uncertainties**. Biometric technologies should not be taken as producing 'the truth' about identity, or as producing absolutely secure border control. As part of the practical configuration of the biometric system, policies and operational procedures would be needed to mitigate the undesirable effects of error rates and threshold flexibility. First, this includes policies and operational procedures on how to deal with biometric errors. It needs to be prevented that users bear the burden to prove that the system made a mistake. This could entail that operators in principle treat a non-match as a false reject, unless there are other doubts about the presented documents/identity claim. For users who do not possess a particular biometric trait, adequate fall-back procedures need to be in place that are no stricter than the initial biometric recognition procedure. Second, boundaries may be put around the possibilities to set and adjust the threshold. This may include regulating the initial setting of the 'acceptable' FAR and FRR for a specific biometric system in a particular context, e.g. the maximum FRR for a set FAR. It may also entail deciding who is allowed to take the decision to adjust the threshold, within which limits, at which level of scale (e.g. for each individual device, for each individual border control point, at national level), and on the basis of what type of information.

Second, **biometric technologies afford a particular distribution of errors and uncertainties.** We have argued how a particular distribution of biometric errors may be the result of normative assumptions about bodies that become inscribed in biometric systems in the design phase. It is important to stress that we do not want to suggest that the designers of biometric technologies (e.g. the algorithm developers) *intentionally* build-in particular tendencies, neither do we suggest that it is easy to locate exactly when and how normative assumptions become built-in, because they are often implicit (see also Introna 2005). In discussing the normative assumptions in biometric technologies, we also do not want to suggest that technologies are more biased than humans. What we do want to problematize is the idea that biometric technologies are objective and value-free. **The crucial point is to acknowledge that biometric system errors are unevenly distributed among different groups of users (Introna 2005).**

In particular when a biometric system is used for border control purposes, **designers and operators need to make sure that the system performs well on a wide range of users**, with different bodily characteristics and behaviours. It needs to be prevented that some people or groups disproportionally experience the consequences of biometric errors. This entails being sensitive to built-in norms and values in capturing devices, matching algorithms, and in the material and practical configuration of the system (e.g. hardware, position of the camera). The aim would be to design, test and operate biometric systems in such a way that they are able to deal with embodied differences in a just and fair way. (see also Introna & Nissenbaum 2009). But system designers and operators not only have a *moral obligation* to guarantee fairness. As we have seen in chapter 2, the operators also have a *legal obligation* to ensure the quality of the biometric data that is processed in a biometric system, and to use biometric systems in such a way that the likelihood of processing incorrect data is as low as possible.

A final challenge is to **guarantee 'equal' recognition results in different circumstances**. The recognition results of biometric systems are dependent on for example threshold flexibility, the operational configurations, and ambient conditions. An important question is to what extent *circumstances* can be allowed to influence recognition outcomes. For example, it would be ethically problematic if for the same person, circumstances (e.g. setting of the threshold/environmental conditions) would produce a non-match at a border control point in Rumania, while at a border control point in Spain other circumstances would lead to a match.

7. Biometrics and (new) practices of information processing

7.1 Introduction

While the previous chapter focused on the process of biometric recognition as such, this chapter focuses on how **biometric systems by translating bodily characteristics into *information* afford (new) practices of information processing**. Such practices include automated processing, categorisation, and the transfer, sharing and linking of data. The issues we discuss below relate to the data protection principles and human rights discussed in chapter 1, but in this chapter we focus on how biometric data processing also brings along various social and ethical challenges and risks, including identity theft, differential treatment of people, covert surveillance, and misuse or unauthorised use of data.

7.2 Biometrics, identity theft and identity fraud

Biometric recognition is generally considered a relatively reliable way of establishing identity, because biological and behavioural characteristics are less easy to manipulate, loose, forget, or share than documents. For this reason, biometric recognition is claimed to be less vulnerable to forgery and identity fraud than traditional forms of identification. **The informatisation of the body however also makes possible specific new forms of identity theft and identity fraud.**

7.2.1 Biometric data and identity theft

In the process of biometric recognition, biometric data in the form of samples and templates get distributed across biometric systems and information networks. The biometrics literature uses the term 'leakage of biometric data' to refer to situations in which the stored biometric information becomes available to an adversary (Jain et al 2011, p. 283). Biometric data may be stored at different locations: in local databases, distributed databases, on ID documents, or on electronic devices. Next to the theft of stored templates or samples, data may also be stolen when it is transmitted (e.g. when template data is sent to the matcher). **The fact that it is *not the body itself, but a digitally constituted and processed dataset* on 'identity' thus generates opportunities for theft, fraud and misuse.**

On the other hand, it is the fact that input data are *derived from bodies* that renders such issues particularly serious. Biometric data are permanently associated with an individual and it is not possible to replace a finger, iris, or face when biometric data are compromised. In addition, when a biometric feature (e.g. a fingerprint) of an individual is compromised, it means that all biometric applications using that same biometric are not secure anymore.

7.2.2 Altering and spoofing biometric characteristics

One form of fooling a biometric system consists of falsifying the biometric characteristic and then presenting this falsified information to the biometric system. An example of this is obfuscation, or the deliberate alteration of a biometric characteristic in order to avoid detection by a biometric system. Obfuscation may include violent acts. Some asylum seekers deliberately damage their fingerprints in order to prevent identification in the Eurodac database for asylum claimants. As a response, in some countries, such as Sweden, a special fingerprint scanner is now used that can read damaged fingerprints (e-Mobidig 2011).

A second example of a strategy to fool biometric systems is ‘spoofing’, in which a user presents an artificial biometric characteristic to the system[27]. Spoofing includes the presentation of a gummy finger or a mask of a face (Jain et al 2011). Contrary to passwords, the body parts that are used in biometric recognition are not secret. Often, remains or copies of a biometric characteristic are available in public as people leave their fingerprints on objects they touch, and photographs of faces can easily be found online. These ‘traces’ can be used for making artificial characteristics with which the system can be spoofed.

7.2.3 Liveness detection

As a countermeasure against spoofing, the biometrics industry has developed liveness detection. Liveness detection involves checking for signs of human vitality or liveness (e.g. blood pulse) so as to differentiate a real biometric characteristic of a user from an artificial characteristic (Jain et al 2011). In the European data protection framework, the principle of data quality (article 6) directs that personal data must by accurate. Liveness detection may improve the accuracy of biometric data as it can detect whether the data are artificial. From a legal and ethical point of view, liveness detection however also requires caution.

First, liveness detection generates additional information about a user. As such it influences the proportionality of data processing of a biometric system. The proportionality principles directs that the processing of the data, its amount and type must be proportional in relation to the interference with the privacy of the data subject. Liveness detection may lead to the processing of greater amounts of data, or of data that are considered sensitive data. Some liveness detection strategies, such as blood pulse or pressure may be revealing of health status, or may generate other unintended information about someone’s emotional state. Pulse rate, for example, may indicate anxiety or stress (Rebera et al 2014). Hence, a higher level of security of a biometric system may cause a loss of privacy for the user (or in legal terms: the data subject).

Second, just like biometric recognition, liveness detection needs to be seen as a process of translation. Similar to biometrics systems, spoof detection systems are also prone to errors (Jain et al 2011) and may for example erroneously indicate that a biometric characteristic is not from a live person. Where it is problematic to view biometric systems as producing ‘the truth’ about identity, it is similarly problematic to assume that liveness detection reveals ‘the truth’ about whether a person is present and alive (also see Pugliese 2014). In addition, we cannot assume that liveness detection itself is immune to spoofing.

7.3 Biometrics and the generation of additional information

In almost any step in the translation of physical characteristic of a body part to recognition result additional information is generated. Especially the captured sample images may include additional information about a person that is not directly needed for performing biometric recognition. **This additional information can be used to improve the performance of a biometric system, but there is also a risk that it consists of sensitive data and/or is used for unintended and unauthorised purposes**.

Additional information may include data that is considered ‘sensitive data’ under Directive 95/46/EC, such as health-related information, or data revealing racial or ethnic origin. Sensitive data could

[27] In border control situations in which the capturing of biometric data is guided or supervised by an officer, spoofing attacks may be more difficult to perform. In this case, officers may also check travellers’ bodies for the presence of artificial materials

potentially be used to discriminate against people. Various biometric modes are claimed to be revealing of health data, including information on illnesses or the likeliness to develop an illness (Mordini & Ashton 2012). In the opinion of the Article 29 Working Party facial images in particular, but fingerprints possibly too, should be regarded as sensitive data as they have the potential to reveal ethnic or racial background (WP 193). In addition, studies have shown that it is possible to predict gender (Lagree & Bowyer 2011), ethnicity (Lagree & Bowyer 2011; Qiu et al 2006), and age (Erbilek et al 2013) from iris texture, while other studies have been successful in estimating gender from fingerprint images (Acree 1999; Badawi et al 2006). While it is obvious that in many cases biometric samples potentially contain additional data, there have not been many studies about additional information in templates. In general, the possibility that biometric templates will contain additional information is much lower compared to biometric samples, but in some cases additional information is likely to be still included in templates (see Kindt & Müller 2007).

Additional information such as gender or ethnicity can help to narrow the search space of potential matches in a database. If, for example, the biometric probe is deemed to be 'Asian Male', the identification database can constrain its search to 'Asian Male' identities only. The additional information can also be used to enable matching. If, for example, a biometric probe of a female user is matched incorrectly against a biometric reference of a male user, the additional gender information can be used to reject the match. Gender, age and ethnicity are also referred to as soft biometrics. Soft biometrics are 'those human characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate between any two individuals (Jain & Kumar 2012, p. 67).

When in an existing a biometric system the function to automatically extract soft biometrics is added, and this information is used as supporting information for identification or verification of a user, *new types of data* are collected. In the European data protection framework, the proportionality principle directs that the processing of the data, its amount and type must be proportional in relation to purpose of the data processing. The new types of data (e.g. gender, age, ethnicity) that are processed may thus influence the proportionality of the processing, especially since they may be considered sensitive data. Under the European data protection directive (95/46/EC) the processing of 'special categories of data' is prohibited. If it is exceptionally allowed, it is subject to specific safeguards[28].

Other types of additional information that biometric systems produce are metadata, which may include the time and place of data processing, the number of attempts to acquire an image, etc. A positive side of this is that it can facilitate accountability and transparency, for example when the actions of border guards and travellers are logged. In case a traveller lodges a complaint about the border check procedures, the logs provide a source of information for assessing the complaint. The logging of location data could also enable the tracking of border guards and travellers. Such data could for example be used to construct evidence by tracking the travel routes of a person suspected of having committed a crime (EES impact assessement).

[28] Article 8 in principle prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. There are however exemptions to this principle, for example when 'the data subject has given explicit consent' (8a), when data processing is 'necessary for the establishment, exercise or defence of legal claims' (8e), or 'by law or decision of the supervisory authority for reasons of substantial public interest' (8:4)

7.4 Biometrics and categorisation

Biometric technologies through enabling the transformation of the body into information also afford categorisation. With biometric data (and additional data), searchable databases can be created. Examples of such databases in the context of border control are the VIS, SIS II and Eurodac. Networked databases have the benefit of allowing quick online searches, but also carry risks. According to David Lyon, a central aim of searchable databases is social sorting: 'to obtain personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on'. The proposed Entry/Exit system for third country nationals provides an example of how biometric and other data can be used to produce profiles and risk categories. One of the aims of this system would be to gather statistics on the entries and exits of third country nationals 'for the purpose of analysis' (EES 2013, p. 40). With this information, it then becomes possible to gain insight into which nationalities and groups of travellers tend to constitute the group of 'overstayers'. In another document, the European Commission suggests that this information can support 'random checks within the territory to detect irregularly staying persons (EC EES impact assessment, p. 16). This would be a clear example of social sorting for differential treatment.

Categorisation does not necessarily lead to discriminatory treatment, but the classifying of biometric and additional data in categories of gender, ethnicity and race can be considered problematic in itself. The categories of race and gender are social constructs and essentially contestable and unstable (Lacqueur 1990; Schiebinger 1993). The classifying of people in categories of race or ethnicity will immediately be challenged by human diversity in the real world. Moreover, even if someone is at one point classified into a particular category, for example as male or female, this may change over time. A clear example are transgender persons whose personal appearance and biometric and personal data are subject to change. The gender classification produced by the biometric system, the gender stated on the ID document, the gender self-identification of a person, and the border guard's interpretation of the person's gender do not necessarily overlap. The resulting gender confusion may cause humiliating and embarrassing situations, especially when it results in increased scrutiny of the person.

7.5 Biometrics and automated processing

Biometric technologies afford the automated recognition of individuals, but this carries the risk of automated decision-making and covert data capture.

7.5.1 Biometrics and automated decision making

Article 15 of the European Data Protection Directive prohibits that a person is subject to automated decisions that produce legal effects concerning them, or significantly affect them, and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to them. Chapter 3 described how biometric processing always affords errors and uncertainty, and how the result of biometric recognition is never 100% accurate. This makes article 15 particularly relevant for automated *biometric recognition.* It means that in border control, operators should not rely solely on biometric technologies, but that these technologies should be used to *support* an authentication process. The decision should not be based solely on the outcome of the biometric verification, but there should be some sort of human intervention before the decision is taken. In other words, when in border control a machine-based system is used for the automated recognition of a person (for example an ABC gate), the final decision to grant someone entry or exit should always lie with the border guard. In addition, if the biometric verification or passport authentication fails, the traveller should be directed to a border guard.

The Directive, however, also states that automated decision-making is allowed when it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests (art. 15, par. 2b). At the same time, this does not exempt the data controller from the legal obligation under article 12a[29] to be able to provide information to the data subject upon his or her request about the logic involved in automated decisionmaking. Yet, because the subject can only request information *after* the data has been processed, the question whether a person is aware that automated profiling has taken place, in particular when this was based on a law instead of on the subject's consent (see also Hildebrandt 2009), becomes crucial.

7.5.2 Covert and distant biometric data capture: 'automatic cooperation'.

Some biometric systems afford the covert and distant data capturing of biometric data. An example of this is the use of facial recognition systems in video surveillance (Introna & Nissenbaum 2009; Introna & Wood 2004). The development of distant sensing can, from one perspective be perceived as convenient and unobtrusive, but from another it represents at least also a significant increase in the extent to which bodies assumed to be available for biometric processing (Van der Ploeg 2012). Moreover, the covert and distant nature of data capture may bring the persons at whom the system is directed in a vulnerable position that contradicts many assumptions embedded in the current discourse on privacy, data protection and user empowerment (Van der Ploeg 2012). The Directive states that the data controller (e.g. the border police) when collecting personal data from a subject must provide the data subject with information on the identity of the controller and on the purposes of processing the data (art. 10a, 10b) In the case of covert capture, there is a risk that this information is not adequately provided.

In short, when biometric systems afford covert and distant capturing of data, people may become less aware, or even unaware of the fact that their body parts are being biometrically processed. In the case of border control, this affects the power relations between the border authorities and the travellers. Distant capturing indicates a decreasing sense of the necessity of actually asking people for their cooperation. As a result, it may become increasingly difficult for travellers to exercise their rights as data subjects and get information about which types of personal data are collected and for what purposes. This threatens various ethical and legal principles, such as that of privacy, self-determination and freedom. Beyond the level of individual rights, it might affect the quality of democratic societies, and the power relations that constitute them (Van der Ploeg 2012, p. 300).

7.6 The transfer, sharing and linking of biometric data

Biometric systems, in particular when they are part of networked systems, afford the transfer, sharing, and linking of (biometric) data, and hence the distribution of biometric data over these networks. The Mobile Pass device is envisioned to become part of networked systems for the management of Europe's external borders (e.g. national databases, SIS II, VIS). This facilitates (real-time) information exchange and allows the checking of databases and watch lists to become a routine practice in border control. The transfer, sharing, and linking of (biometric) data on the one hand makes border control more secure, but on the other hand carries risks for the data subjects.

[29] Article 12 a: Member States shall guarantee every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

David Lyon has coined the term ‘data doubles’ to refer to virtual identities located in networked databases (2008, p. 30). He argues that these data doubles have ‘far greater rates of mobility than their real-life counterparts’ (idem, p. 29). Where these data doubles are located, and with what agencies they are shared, are important questions. The persons whose personal data get distributed in networked databases may lose control over their data, and not know where they are transferred to, and by whom they are used.

The distribution of biometric data also carries the risk that the data are used by new actors in possibly unauthorised ways. As we have seen in section 7.2, stored biometric data may leak, be misused, or manipulated. Even if access to networked databases is regulated by law, this does not prevent the extension of access to new authorities or countries in the future. The SIS, for example, originally was only accessible to police and border authorities, but can now also be accessed by asylum authorities and Europol. And while EURODAC was set up for managing responsibilities for asylum applications, the new EURODAC regulation allows access to law enforcement agencies and EUROPOL for the purpose of preventing, detecting and investigating terrorist activities and serious criminal offences. This shows how the issue of access is related to the risk of function creep: the gradual widening of the use of the database beyond the purpose for which it was originally intended. In addition, when access to the information contained in databases is granted to other countries, the data are no longer protected by the data protection regimes of the originating country. If access is granted to third countries that have weaker data protection principles, this can have potentially negative effects for the data subject.

Another aspect of networked databases is that biometric data can potentially be linked with other data in other databases, thereby allowing identification, classifications and profiling (see also 4.4.) Hence, the transfer, sharing and linking of biometric data should not be understood in terms of potential violation of privacy or data protection principles only. Biometric data in border control are used to facilitate or impede the movement of people across borders, and what happens to these data hence affects people’s life-chances and choices (Lyon 2003).

7.7 Conclusion

Biometric systems afford (new) practices of information processing that may bring along undesirable effects, such as misuse or unauthorised use of biometric data. In addition, processing practices may lead to automated decision making, entail covert and distant capturing, or enable categorisation and profiling. To mitigate the (potential) risks associated with these processing practices, it is important that designers, implementers, and operators of biometric systems provide safeguards and protections for the processing of biometric data.

First, because biometric identity theft has very serious consequences for the victims, but also for the reliability of the biometric system and on a more general level for public trust in authorities, **a high level of security of processing is required.** The data protection principles discussed in Chapter 2 provide guidelines for secure processing. An example of a protective measure would be to encrypt biometric data when they are transmitted between the MobilePass device and the databases or servers to which it is connected, and to only use highly secure connections.

In addition, and in line with data protection principles, **biometric data should only be stored on the device or a server if this is absolutely necessary** and also not be stored longer than necessary. In addition, biometric data should be stored separately from other identifying information. If data are stored, there should be strict rules on who has access and under which conditions. The lightness, smallness, and detachability of the MobilePass device may become a liability as it renders the device more vulnerable to theft and loss as compared to fixed computer systems. Therefore, it is important that procedures are in place to guarantee that only authorised operators have access to the device.

Yet, it is important to understand the storage of data not only in terms of potential violations of data protection principles: **the storing of data can also enhance transparency and accountability**. Examples of this are the logging of anonymous operational data for quality control and performance assessment, but also the logging of operator ID, and network communication for monitoring the security of processing.

The **processing of facial images by the MobilePass device requires special attention**, because facial images can in some contexts be considered sensitive data. The same is true for some types of data that are used in liveness detection. In general, it needs to be prevented that these potentially sensitive data are used for other purposes than identity authentication.

When capturing 'at a distance' takes place, there is the risk that people are not aware that their data are being processed. This goes against the principle of fair processing, and at a more general level it leads to a shifting of power relations between the authorities and the traveller by placing the traveller in a more vulnerable position. **This means that with touchless fingerprint capturing, and with video-based facial image capturing in particular, the operators need to make sure travellers are aware that capturing takes places, for example by asking for their cooperation**. In addition, should the device afford covert capturing, this should not be done for unauthorised purposes, such as the tracking of people (or any purpose beyond verifying the identity of travellers as part of checks at the external border).

Automated decisionmaking needs to be prevented by making sure that operators do not rely solely on results produced by the device. Because the configuration of the MobilePass device as a handheld device *assumes* the presence of a border guard, the risk of automated decisionmaking is smaller than in configurations such as ABC gates. Nevertheless, chapter 3 already indicated that operators should not put too much trust in a technology that affords errors and uncertainty. The display of the device could be designed in such a way that operators are stimulated to 'assess' the recognition result, for example by having the biometric recognition result displayed not as a simple 'yes' or 'no', but as a similarity score.

8. The emergence of the 'portable biometric border'

8.1 Introduction

Borders are generally understood as fixed, permanent lines separating different territories. Social scientific approaches, however, stress that borders only get meaning when they are *performed* by border guards and border crossers. This also entails that borders are not necessarily at the edges of the nation-state, but can also be found within societies, for example in cities (idem). In this chapter we take as a starting point that 'the border' materialises wherever border practices take place (Johnson et al 2011). This allows us to see how handheld biometric devices enable the performance of the border at different sites.

A biometric system as part of a handheld device for border control affords the 'portability' of the networked biometric border: the border becomes 'attached' to border guards' individual bodies, but at the same time the border potentially shifts to new places and times. Portable borders thereby allows new ways of managing and controlling people's movement across borders.

This chapter discusses social and ethical aspects related to the 'portable biometric border'. It does so by placing mobile biometric devices in the context of a wider development of borders becoming 'mobile'. It also analyses how biometric technologies have become enrolled in political programmes of 'smartening up' Europe's external borders. The chapter ends with a discussion of the particularities of land borders, the challenges they pose to biometric border control, and the ways in which mobile biometric devices would transform the workings of land borders.

8.2 Portable devices and mobile borders

Technology has been argued to facilitate the 'decoupling of functions traditionally attached to the frontier from the actual territorial border' (Dijstelbloem & Broeders 2014, p. 4). Networked databases make it possible to check a person's visa application history at a consulate abroad, but also to identify a (potential) illegal migrant during a traffic control in a city. **Biometrics play an important role in the proliferation of the border, because they can be viewed as 'inscribing' the border on peoples' bodies** (Van der Ploeg 2005; Amoore 2006). 'By virtue of the ever closer link established by networked databases and biometrics between persons and their registered identity, the border becomes more than ever part of the embodied identity of certain groups of people, verifiable at any of the many points of access to increasingly interconnected databases. Biometrics thereby enable the extension of the function of the border beyond the actual geographical line to places both outside the territory of a nation-state and inside the country' (Van der Ploeg 2006, p. x).

Portable devices further extend the biometric border. The use of portable devices allows the authorities to collect and process biometric data away from fixed locations (e.g. border crossing points). Portable devices also make possible border checks on persons *en route*, for example inside means of transportation such as buses and trains. Mobile biometric devices connected to networked databases therefore amplify the shifting of the biometric border: biometric border checks can potentially take place wherever persons and authorities meet.

The 'shifting' of the border brings up several legal and ethical issues. The legal basis for conducting border checks in third countries is often not clear, especially when third countries or non-state actors such as airlines, play a role in such border control practices. An important concern is that 'extra-territorial' checks may violate the right to asylum (art 18. EUCFR). Under Article 3(1) of the Dublin Regulation (Regulation (EU) No. 604/2013) EU Member States are required to examine any application for international protection lodged by a third-country national or a stateless person. An individual can only apply for asylum when he/she is on the territory of the EU, or has arrived at the border (including shared border control points, territorial waters and transit zones). This means that if border authorities identify a person before he or she arrives at 'the border', for example when people are intercepted on the high seas, or at airports abroad, the right to asylum may be violated. This is ethically problematic, because most people who wish to seek asylum in the EU are nationals of countries requiring a visa to enter the EU. Potential asylum seekers often do not qualify for an ordinary visa, or choose not to apply because they fear the authorities in their country will find out they want to leave the country. This means they may decide to cross the border with forged documents. When they are intercepted at high sea or denied boarding at the airport of departure, they have never arrived at the European border and hence cannot apply for asylum. While these examples may seem to have little to do with the foreseen use of the MobilePass device, it is important to be aware of extra-territorial border control practices. The portability of mobile biometric devices makes them potentially attractive technologies for conducting such legally and ethically contested border control practices.

8.2.1 The portable border attached to border guards

With handheld devices, the border becomes 'attached' to border guards' individual bodies. **Handheld biometric devices thus afford the 'portability' of the networked biometric border in a very literal sense.** This portability transforms the workings of the border in several ways: it entails a particular scripting of the ways which both travellers and border guard interact with the device, and it changes the relations between travellers and border guards.

A handheld device requires a particular availability of the bodies of both the traveller and border guard. The MobilePass device is envisioned as consisting of three components: a full-page passport reader, a device for display, control & input, and a camera for capturing fingerprint and facial images (the MobilePass reader). The border guard wears the passport reader on the hip, while the device for display, control & input and the camera are wrist-worn. The wrist-worn camera can be detached and operated with one hand, and will weigh 1 kg maximum. The device requires the border guard to perform particular physical movements (placing the passport in the hip-worn passport reader, detaching the camera from the wrist, bringing it within capturing distance of the traveller's body, not moving the camera too much, re-attaching it, reading results from the display, entering data etc). The traveller is required to be within capturing distance of the device (80-200 cm for face, 10-12 cm for fingerprints), and to present her face and fingers in a particular way (open hand). An important question for the user acceptability is how in a particular socio-material configuration travellers and border are expected to perform specific parts of these 'choreographies'. Who, for example, needs to move to bring body parts within various capturing distances?

The handheld character of the device may also transform relations of power between traveller and border guard in various ways. Depending on the number and type of actions that are logged, the physical attachment of the device to the border guard may entail increased accountability and surveillance of border guards. In addition, a scanning device that is attached to a border guard requires close physical interaction between traveller and border guard. If the device prescribes that the border guard holds the camera (instead of passing it to the traveller), this requires the traveller to be physically close to the border guard (10-12 cm for fingerprint). It is important to investigate how this may change the way travellers experience being checked. For example, there may be a chance that the close physicality required for fingerprint scanning in particular generates an experience of handheld biometric border control as 'increased scrutiny' rather than as 'facilitated passage'. It may well be that in ABC for EU travellers, it is the *automated* character of ABC gates, or in other words, the *absence* of border guards that is a crucial part of the experience of facilitation.

Another example would be that devices that work with remote capturing technologies (fingerprint in particular) may invoke an image of 'barcode scanning' of travellers. Finally, a scanner that is designed with a grip may induce associations with handguns and thus be experienced as intimidating.

8.3 Biometrics as part of political programmes

Biometric technologies are introduced for specific purposes, such as improving the efficiency of border management, or improving the security of identification. This section focuses on **biometric technologies as part of specific political programmes for the management of (cross-border) movement**. It discusses the aspirations surrounding three future political programmes that together form the new European strategy of external border management: the Entry-Exit system, the Registered Traveller Programme, and Automated Border Control. The EES and RTP for non-EU travellers, and ABC for EU travellers, will transform the ways in which peoples' movement across borders is managed and controlled. Embedded in these programmes are aspirations that the programmes produce certain types of outcomes, and particular ideas about biometric technologies as enablers of 'security', 'facilitation', and 'convenience'. It is important to discuss these aspirations and expectations for two reasons: First, the three specific programmes (EES, RTP, ABC) shape expectations about the role of biometrics in border control in general. Second, and on a practical level, the MobilePass device may in the future become one of the technical instruments used in the execution of one or more of these programmes.

8.3.1 Imagining the role of biometrics in the EES, RTP and ABC

In recent years, the management of the European external border began to be viewed not only as a security problem, but also in terms of mobility. With the increased volumes of travellers at the external borders, the EU saw a need to move towards 'modern and efficient border management by using state-of-the-art technology' (European Commission, 28-02-2013). 'Smart borders' would speed up border check procedures for third country nationals entering the EU while at the same time enhancing security, thereby ensuring that 'the EU remains open to the world and attractive as a destination for non EU-travellers' (ibidem). The proposals for an Entry/Exit system and a Registered Traveller Programme are the result of these new approach. A related development is the encouragement by the European Council for Member States to introduce and use automated border control for EU travellers more extensively, based on the biometric passport (see Chapter 3).

In European policy documents, biometrics feature as a core technology enabling the 'smartening up' of European borders. In both the proposal for the EES and the RTP the use of fingerprints and facial images is foreseen, but the discursive justification for using biometrics and the actual material and practical configurations of which they would become part, differ. **The use of biometric technologies as part of the EES is justified mainly by presenting biometrics as a reliable means to establish an identity.** Biometrics are claimed to be helpful in 'preventing identity fraud' (EES impact assessment p. 34), 'identifying irregular migrants within the territory who are no longer in possession of their travel documents' (p. 27), and 'establishing the identity of a person who is a crime victim or of a person who is suspected of having committed terrorist offences or other serious criminal offences' (p. 28).

In EC documents on the RTP, the reasons for using biometrics are hardly explained. Here, it seems that biometrics are simply *assumed* to be a necessary component of automated border control. Biometric technologies seem to be introduced for their capacity to automate the identity authentication process instead of their capacity to make it more reliable. Related to this is that the RTP is framed in terms of speed and convenience, much more than in terms of security. Similarly, in the European Council's document on ABC for EU travellers, the use of biometrics-based ABC is framed almost completely in terms of facilitation and speed.

8.3.2 Problematising 'speed' and 'facilitation' in automated biometric border control

The idea that automated border control with the help of biometrics 'facilitates', and 'speeds up' the border process, can be questioned. It is often assumed that travellers pass automated gates faster than manual checks, but official numbers indicate that at airports EU travellers on average need 15-20 seconds at an ABC gate, while a manual check for this group on average takes 10-15 seconds (Oostveen et al 2014; RTP impact assessment). In addition, empirical research has shown that the 15-20 seconds processing time per ABC gate is based on 'perfect' border crossing, and not on the average traveller's behaviour at an ABC gate (Oostveen et al 2014). It also does not take into account biometric errors due to, for example, bad templates in e-passports (Spreeuwers et al 2012). Also, the 'speed' that automated border control produces is potentially reduced as a result of lack of space. At many border crossing points, space is a scarce resource and the number of ABC gates that can be installed is limited. Furthermore, if we consider the time it takes to pass a border to include not just the border checks, but also the queuing, yet another picture emerges. It appears that the benefit of using ABC is mainly due to the fact that the queues are shorter here, because not many people use them yet (EC PWC study). Finally, the 'speeding up' that the RTP would offer to registered TCN is not a direct effect of the automated character of the checks, but an effect of the abolishing of eligibility questions. Because these travellers will have been pre-screened, the legal obligation to verify their travel plans, financial means etc. as part of the thorough check at the border no longer applies.

All this shows that biometrics-based ABC does not automatically lead to speedier border passage, but that this also depends on the particular socio-material configuration of which it is part, and the environment in which it is used. It is questionable if biometrics-based ABC gates for EU and 'low risk' TCNs can still be presented as 'facilitating' and 'speeding up' border passage once their use becomes more widespread. If the main justification for introducing biometrics-based ABC for EU travellers and registered travellers is that it facilitates and speeds up border passage, this has important legal and ethical consequences. The Frontex ABC guidelines also bring this to the fore:

> Bearing in mind that automated border checks are currently targeted to EU citizens (for which only minimal checks are required as per the Schengen Borders Code), the primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met. This situation may change in the future if it is decided to open the use of ABC systems to third country nationals (TCN) carrying electronic travel documents and/or electronic Visas. Since TCNs may pose a different risk than EU citizens, the trade-off between security and facilitation is likely to be a different one.

As we have seen in chapter 1, the collection of biometrics is considered an interference with the right to respect for private and family life, and the necessity and proportionality of using them therefore need to be demonstrated. It might become challenging to positively demonstrate this when biometrics-based ABC for EU travellers and/or TCNs does not actually achieve the aim of 'facilitating' border passage.

8.3.4 Implications for Mobile Pass

There is a dominant discourse that 'new technologies', including biometrics, can 'speed up' border passage while at the same time making it 'more secure'. However, the actual realisation of these objectives is not straightforward. What is clear is that the MobilePass device may become part of specific political programme (EES, RTP, ABC) which have different desired main objectives: facilitation (ABC, RTP) OR security (EES).

This entails that dominant discourses on the use of biometrics in programmes for the management of movement should not be copied unreflexively for justifying the development and implementation of the MobilePass device. In addition, what is needed is careful evaluation, for example during the MobilePass demonstration phase, of the actual realisation of desired outcomes.

8.4 Smart borders, biometrics, and the production of identities

Some authors argue that instead of being mere descriptors of identity, biometrics can also be understood as being constitutive of identities. Such approaches seek to understand how biometrics are part of particular uses and practices of establishing an identity (Van der Ploeg 2005). In this line of reasoning, the traveller as a subject is 'not always and already there awaiting identification but rather is produced by particular practices' (Ruppert 2011). The practices of the Entry/Exit system, for example, can be understood as producing 'potential illegal migrants' or 'potential overstayers'. The EES, in storing the fingerprints and facial images of TCNs together with the date of entry in a central database, produces TCNs as subjects whose movements need to be surveilled and controlled. Similarly, the proposed collection of all 10 fingerprints of TCNs in the EES and the foreseen access of law enforcement to the database constitutes TCNs as 'potential suspects'.

The smart borders proposal has also been criticized for the terminology used in the proposals in which members of the RTP are called 'low risk' or 'bona fide' travellers. The EP was concerned that this could imply that TCNs who are not members are considered 'high risk' or 'mala fide'. The EDPS warned that:

> '[t]here may be a risk of discrimination as only the travellers taking specific steps through ad hoc registration and provision of detailed information would be considered 'low-risk' travellers while the vast amount of travellers who do not travel frequently enough to undergo such a registration or whose fingerprints are unreadable, would thus, by implication, de facto be in the 'higher-risk' category of travellers' (EDPS 2013, p. 20)

While the EC's RTP impact assessment emphasises that 'those not using the ABC are not considered as more risky travellers', it has also been argued that the move towards border management on the basis of risk analysis and profiling stands in a difficult relationship with the principle of non-discrimination (Carrera and Hernanz 2014). The European Economic and Social Committee for example stressed that 'the potential use of race, ethnicity or other sensitive grounds as a basis for statistical dataveillance is difficult to reconcile with non-discrimination principles, secondary legislation and fundamental rights obligations' (EESC 2013 OJ C 271/99).

A general ethical concern is that the area of freedom, security and justice is an area characterised by unequal mobility rights for TCNs and EU citizens. With the increased use of biometrics and their storage in databases such as VIS, SIS, Eurodac and possibly the EES, border checks on TCNs at entry as well as the monitoring of their movement within Europe are intensified. This not only produces different images of TCNs and EU citizens, but it could be argued to also reinforce existing mobility inequalities.

8.5 Land borders

Because mobile biometric devices are expected to be particularly useful devices for conducting checks at land borders, and are already used in that context, this section discusses some of the particularities of land borders. Land border crossing points (BCPs) and the check practices at land BCPs vary widely, due to for example differences in traveller flows (busy BCPs vs quiet BCPs), and type of transportation (road BCPS, rail BCPs). In general, land BCPs constitute much less controlled environments than air BCPs (Frontex ARA 2014). These factors affect the performance of mobile biometric devices, bringing along various social and ethical issues.

8.5.1 Traveller flows at land BCPs

A study commissioned by the EC calculated that in 2014, around 23% of external border crossings took place via land borders (refer). European land borders show a different composition of the traveller flow when compared to air borders: at land borders the percentage of visa holders is 41%, while at air borders this is only 14% (see table 1). **This means that at land borders relatively more thorough checks need to be conducted, including the mandatory biometric verification of visa holders.**

	Air	**Sea**	**Land**	**Total**
	Entry and exit	*Entry and exit*	*Entry and exit*	*Entry and exit*
EU	**265**	**36**	**71**	**372**
Visa Exempt TCN	**68**	**7**	**6**	**81**
Visa Holding TCN	**52**	**5**	**54**	**110**
Total	**385**	**48**	**131**	**564**

Table 1) border crossings at the external borders of the Schengen Area for 2014 (in millions)[30] (based on PWC 2014, p. 309)

8.5.2 Environmental conditions at land BCPs

Another characteristic of land borders is that (a part of) the checks may take place in an outdoor environment. The environmental factors at European land borders vary greatly: there are geographical and seasonal differences in temperature, weather conditions, duration of daylight, etcetera. **These highly dynamic and to a large extent uncontrollable conditions may influence the performance of biometric devices**, for example by affecting the quality of the acquired biometric samples (and hence data accuracy). The capacity of mobile biometric device to produce **'equal' recognition results in different ambient conditions** is therefore a technical challenge with important ethical impact: it would be ethically problematic if ambient conditions to a large extent influence whether or not a match or non-match is produced.

8.5.3 Border checks at land BCPs: roads and railways

A mobile biometric device, because of its portability and connectivity, affords checking *inside* means of transportation, for example in cars, buses, and trains. It also potentially could be used to conduct border checks at shared BCPs outside European Union territory.

The Schengen Borders Code specifies how border checks at land borders need to be carried out. It states that at land border control points, different lanes can be installed for checking passengers with

[30] For the PWC study all entries and exits at the external borders of the Schengen Area (with the addition of Bulgaria, Croatia, Cyprus and Romania) were recorded during one week, from 12 to 18 May 2014. The results obtained were extrapolated for one year.

European and non-European passports. It also stipulates that "[a]s a general rule, persons travelling in vehicles may remain inside them during checks. However, if circumstances so require, persons may be requested to alight from their vehicles. Thorough checks [i.e. second line] will be carried out, if local circumstances allow, in areas designated for that purpose." **A mobile biometric device because of its portability and network connections would enable the checking of persons inside vehicles**. While this would make the checking process more convenient for travellers, the environmental condition of the vehicle may also influence the data quality of captured biometric samples (e.g. position/movement of user, lighting etc.).

The Schengen Borders Code contains additional rules for checking train passengers entering or exiting the territory of the European Union. It allows checks on train passengers to take place on board the train between the last station of departure in the third country and the first station of arrival at the territory of the Member State (or vice versa). It also allows checks at the last station of departure on the territory of the neighbouring third country. For high speed passenger trains, even checks at/between all stations on the itinerary –both in the third country and on the territory of the Member States, are allowed by common agreement with the third country. Member States are also allowed to use secure connections to access information systems such as SIS-II for these checks. **Mobile biometric devices 'activate' these legally allowed potentialities: allowing for biometric database checks 'en route', they enable the extension of the external EU border along the complete travel route of the train in the third country and on European territory**.

While conducting checks inside means of transportation is often assumed to increase the speed and convenience of border crossing for travellers and decrease the logistical pressure at the BCP, there may also be (practical) problems. Conducting border checks inside moving trains, for example, makes these checks to some extent dependent on the temporalities of the train journey. This could lead to time pressure as border guards will need/want to have finished the checks when the train enters the first station at the territory of the EU. Another point of concern would be how to deal with those travellers selected for second line checks or wanted persons, as the number of border guards on board the train will probably be limited. A final complicating factor for border control taking place inside trains and buses, is that EU travellers and TCNs are mixed. This means there are no possibilities to separate these travellers in different lanes or queues (EU travellers and non-EU travellers). This may make it more difficult to organise the checking process efficiently.

8.6 Conclusion

Mobile biometric devices through their portability and connectivity (as compared to fixed computer systems) significantly expand the number of possible sites for conducting biometric border checks. The proliferation of the biometric border, however, brings up several social, legal and ethical issues,

This chapter discussed several examples of legally contested extra-territorial border control practices in which mobile biometric devices could potentially be used, such as document checks by airlines at the airport of departure. Mobile biometric devices may also potentially be used inside the EU when internal border checks are temporarily reintroduced in the case of a serious threat to public policy or internal security. Moreover, if mobile biometric devices would be adopted not just for conducting border checks, but also by other authorities that conduct identity checks in public spaces within EU territory (e.g. immigration and police services), (biometric) identity checks may become even more ubiquitous.

Those developing and implementing handheld biometric devices need to be aware that the particular design of a device always to some extent prescribes how it should be used. This not only structures the interactions between the device and its users (border guard and traveller), but may also transform relations *between* travellers and border guards.

Governments who implement mobile biometric devices need to pay particular attention to proving the necessity and proportionality of using biometrics. When used as part of the minimum check on EU citizens in particular, the dominant idea that biometrics ‘facilitate’ and ‘speed up’ border crossing may be misleading.

Other social and ethical issues arise when biometric devices become part of the EU’s political programmes for the management of movement. Biometrics as part of different border control practices for EU travellers and TCNs thereby contribute to the production of different ‘traveller identities’: EU travellers as low risk travellers (whose border passage needs to be facilitated), and TCNs as ‘potential overstayers’ and even ‘potential criminals’ (whose movement within the territory of the EU needs to be monitored).

Finally, the performance of mobile biometric devices in the highly diverse and largely uncontrolled environment that land borders represent, is an issue of concern. The devices will a.o. need to be able to deal with the large variation in environmental conditions, different types of travellers (in terms of their status as EU or non-EU traveller), and diverse logistical challenges at (mobile) land borders. Designers and vendors will need to be clear about the possibilities and limitations of biometric technologies in such environments.

Bibliography (incomplete)

Acree, M. A. (1999). Is there a gender difference in fingerprint ridge density? *Forensic Science International, 102*(1), 35-44.

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

Badawi, A., Mahfouz, M., Tadross, R., & Jantz, R. (2006). Fingerprint-based gender classification. *Proceedings of the 2006 International Conference on Image Processing, Computer Vision, & Pattern Recognition, Las Vegas, Nevada, USA, June 26-29, 2006, Volume 1,* 41-46.

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

De Hert, Paul.,Riehle, Cornelia.,. (2010). Data protection in the area of freedom, security and justice : A short introduction and many questions left unanswered. *ERA-Forum : Scripta Iuris Europaei, 11*(2)

Dijstelbloem, H., Broeders, D. (2014). Border surveillance, mobility management and the shaping of non-publics in europe. *European Journal of Social Theory,* , 1368431014534353.

Erbilek, M., Fairhurst, M., & Abreu, M. (2013). Age prediction from iris biometrics.

Hayes, Ben.,Vermeulen, Mathias.,. (2012). *Borderline the EU's new border surveillance initiatives : Assessing the costs and fundamental rights implications of EUROSUR and the "smart borders" proposals : A study by the heinrich Böll foundation*. Berlin: Heinrich-Böll-Stiftung.

Howard, J. J., Etter, D. (2013). The effect of ethnicity, gender, eye color and wavelength on the biometric menagerie. *Technologies for Homeland Security (HST), 2013 IEEE International Conference on,* 627-632.

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

Introna, L. D., Nissenbaum, H. (2009). Facial recognition technology: A survey of policy and implementation issues. *Center for Catastrophe Preparedness and Response, New York University,*

Introna, L., Wood, D. (2002). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society, 2*(2/3)

Jain, Anil K., Ross, Arun A.,Nandakumar, Karthik,. (2011). Introduction to biometrics.

Jain, Anil K., Kumar, Ajay,. (2012). Biometric recognition: An overview. *Second generation biometrics: The ethical, legal and social context* (pp.xx) Springer

Johnson, C., Jones, R., Paasi, A., Amoore, L., Mountz, A., Salter, M., & Rumford, C. (2011). Interventions on rethinking 'the border' in border studies. *Political Geography, 30*(2), 61-69.

Kindt, E., & Müller, L. (2007). D3. 10: Biometrics in identity management".

Lagree, S., & Bowyer, K. W. (2011). Predicting ethnicity and gender from iris texture. *Technologies for Homeland Security (HST), 2011 IEEE International Conference on,* 440-445.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination* Psychology Press.

Lyon, D. (2008). Filtering flows, friends, and foes: Global surveillance. *Politics at the Airport,* , 29-50.

Martin A.K., Whitley, E. A.,. (2013). Fixing identity? biometrics and the tensions of material practices. *Media Cult.Soc.Media, Culture and Society, 35*(1), 52-60.

Mordini, E., Ashton, H. (2012). The transparent body: Medical information, physical privacy and respect for body integrity. *Second generation biometrics: The ethical, legal and social context* (pp. 257-283) Springer.

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

Oostveen, A., Kaufmann, M., Krempel, E., & Grasemann, G. (2014). Automated border control: A comparative usability study at two european airports. *8th International Conference on Interfaces and Human Computer Interaction (IHCI 2014), Lisbon, Portugal,*

Phillips P.J., Jiang F., Narvekar A., Ayyad J., & O'Toole A.J.,. (2011). An other-race effect for face recognition algorithms. *Trans.Appl.Percept.Transactions on Applied Perception, 8*(2)

Prins, C.,. (1998). Making our body identify for us: Legal implications of biometric technologies. *Computer Law and Security Review: The International Journal of Technology and Practice, 14*(3), 159-165.

Pugliese, J.,. (2007). Biometrics, infrastructural whiteness, and the racialized zero degree of nonrepresentation. *Boundary 2., 34*(2), 105.

Pugliese, J.,. (2014). The alleged liveness of “Live”: Legal visuality, biometric liveness testing and the metaphysics of presence.

Qiu, X., Sun, Z., & Tan, T. (2005). Global texture analysis of iris images for ethnic classification. *Advances in biometrics* (pp. 411-418) Springer.

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

Rebera, A. P., Bonfanti, M. E., & Venier, S. (2014). Societal and ethical implications of anti-spoofing technologies in biometrics. *Science and Engineering Ethics, 20*(1), 155-169.

Rebera, A. P., Guihen, B. (2012). Biometrics for an ageing society societal and ethical factors in biometrics and ageing. *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the,* 1-4.

Ruppert, E. (2011). Population objects: Interpassive subjects. *Sociology, 45*(2), 218-233.

Van der Ploeg, I. (2005). *The machine readable body : Essays on biometrics and the informatization of the body*. Maastricht: Shaker Pub.

Van der Ploeg, I., Sprenkels, I. (2011). Migration and the machine-readable body: Identification and biometrics. In H. Dijstelbloem, & A. Meijer (Eds.), *Migration and the new technological borders of europe* (pp. 68-104). Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Van der Ploeg, I.,. (2012). Security in the danger zone: Normative issues of next generation biometrics. *Second generation biometrics: The ethical, legal and social context* (pp. xx) Springer

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