Chapter 2
An Introduction into the Use of Biometric Technology

2.1 A Long History of Use of Biometric Characteristics

2.1.1 The Use of Biometric Characteristics in Ancient Times

27. The idea that parts of our body can be used to identify our unique selves is not new. Prints of hand, foot and finger have already been used in ancient times because of their unique characteristics.

28. In caves in France, discovered by the group of Chauvet, paintings believed to be created by *prehistoric men* and estimated to be around 32,000 years or even 36,000 years old, contained handprints. Some of these prints are believed to have been fixed by the originators of the images to identify themselves.[1]

29. The Babylonian King Hammurabi (1792–1750 BC) is known to have enacted one of the first written codes of law in the world in clay tablets. The kings of Babylon were supposedly using an imprint of their right hands in the clay tables in order to authenticate the tables.[2] In *Babylonia*, fingerprints were also used in business transactions that were recorded on clay tablets.[3]

[1] See J. Clottes, *Chavet Cave* (*ca. 30,000 B.C*), The Metropolitan Museum of Art, available at http://www.metmuseum.org/toah/hd/chav/hd_chav.htm

[2] See J. Ashbourn, *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies*, DG JRC – Seville, European Commission, January 2005, p. 4, ('Ashbourn, Social Implications of Wide Scale Implementation of Biometrics, 2005'), available at http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf

[3] See Biometrics Task Force, *Biometrics History Timeline*, slide 1, Department of Defense (U.S.A.), available at http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx ('Biometrics Task Force, Biometrics History'). About the richly documented Babylonian culture, see also M. Jursa, *Die Babylonier*, München, Beck, 2004, 128 p.

E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Law, Governance and Technology Series 12,
DOI 10.1007/978-94-007-7522-0_2, © Springer Science+Business Media Dordrecht 2013

30. Chinese use fingerprints and handprints as marks of authenticity for at least 2,000 years. In ancient *China*, fingerprints were routinely pressed in clay tablets and clay seals. Documents from the Tang dynasty in China (618–907) referred to the use of fingerprints and handprints on contracts.[4] Others report that Chinese merchants used in the fourteenth century palm and footprints to distinguish children from one another.[5]

2.1.2 The Scientific Study of Fingerprint, Anthropometry and Dactyloscopy since the Seventeenth Century

31. A few centuries later, an English plant morphologist, Dr. Nehemiah *Grew*, published in 1684 about the ridges on human hands and feet. A Prussian professor of anatomy and physiology Johannes *Purkinje* illustrated nine fingerprint pattern types in his work in 1823 and classified for the first time fingerprints. A Scottish physician and surgeon Dr. Henry *Faulds* who practiced in Japan published as one of the first work proposing that the ridge detail of fingerprint is unique and can prove identity by comparison with marks found at the scene of the crime.[6]

32. In the British Indies colonies, Sir William *Herschel*, working as a British officer for the Indian Civil Service, started in the 1850s putting signatures of the hand and fingerprints on contracts. The prints were used in order to avoid that workers were paid twice or that one would impersonate someone else upon pay day. He is often credited with being the first European to recognize the importance of fingerprint for identification.[7]

---

[4] A. Farelo, *A History of Fingerprints*, Interpol, April 2009, p. 2, available at http://www.interpol.int/Public/ Forensic/fingerprints/History/BriefHistoricOutline.pdf ('Farelo, A History of Fingerprints, 2009').

[5] See Z. McMahon, *Biometrics*: *History*, Indiana University, Indiana University Computer Science Department cited in National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, 7 August 2006 (updated), p. 1, ('NSTC, Biometrics History, 2006'), available at http://www.biometrics.gov/Documents/BioHistory.pdf. The author referred to writings of the explorer Joao de Barros.

[6] R. Develtere, 'Dactyloscopie: grandioos verleden, wat met de toekomst ?', in W. Van de Voorde, J. Goethals en M. Nieuwdorp (eds.), *Multidisciplinair forensisch onderzoek*, Brussel, Politeia, 2003, (317), pp. 317–318 ('Develtere, Dactyloscopie, in Van de Voorde, Goethals and Nieuwdorp, Multidisciplinair forensisch onderzoek, 2003').

[7] See also B. Laufer, 'History of the finger-print system', *1912 Smithsonian Institution Annual report*,1912, reprinted in *The Print*, vol. 16 (2), 2000, pp. 1–13 and available at http://www.scafo.org/library/160201.html; M. Triplett, *Michele Triplett's Fingerprint Terms. A collection of over 900 terms used in the Science of Fingerprint Identification*, 20 December 2008, available at http://www.fprints.nwlean.net/index.htm.

33. Adolphe *Quetelet*, a Belgian astronomer and mathematician, was one of the founders of the science of anthropometry and biostatistics in the early nineteenth century. *Anthropometry* is the study of the measurement of various anatomical traits.[8] In 1871, Quetelet published *Anthropométrie ou Mesure des différentes facultés de l'homme*. While using the Gauss curve, he advanced that the data of the biometric characteristics of persons vary around averages and seem constant.[9]

In France, Alphonse *Bertillon* of the police in Paris introduced the concept of *judiciary anthropometry* (i.e. the use of body measurements) and the use of marks on bodies to identify criminals, also called Bertillonage, largely used by the French police since 1882.[10] Others adopted the principle as well, even though this was not at that time a well proven technique.[11]

34. Dactyloscopy is the study of the fingerprints. These prints were in the nineteenth century (until sometimes nowadays) taken as ink patterns. Abandoning the Bertillonage, it was practiced and promoted by an Argentinean police official and anthropologist, Juan *Vucetich*, who in addition published *Dactiloscopia Comparada*, a study on comparative dactyloscopy.[12]

35. In the 1890s, Sir Francis *Galton*, explorer and scientist, also studied the unique characteristics of fingerprint. He demonstrated that each individual has *unique* fingerprints which remain persistent during a whole life.[13]

36. Scotland Yard soon discovered the success of the use of fingerprints to identify criminals and adopted the use of fingerprint since 1901, when a new bureau for

[8] By analyzing the measurements relating to height, weight and size of the breast of French draftees and of 5.738 Scottish soldiers, Adolphe Quetelet applied the rules of probability on the biometric data of human beings. He was also one of the founders of modern statistics. See (Belgian) Federal Government Services Economy, *Adolphe Quetelet* (*1796–1874*), available (in Dutch) at http://www.statbel.fgov.be/info/quetelet_nl.asp

[9] He developed the model named by him the 'curve of the possibilities' and created the concept of the 'average person'. In his work '*Sur l'homme et le développement de ses facultés*; *Essay d'une physique sociale*', published in 1835 (of which a second edition as 'Physique sociale' appeared in 1869) he studied the rules which determine a human being from a physiological, intellectual and moral perspective. The application of the concept of the 'average person', not only upon the physical characteristics, but also for determining the intellectual and moral qualities of person, however, was criticized. The Quetelet-index (or Body Mass Index) by which the ideal weight of a person can be determined, is still used in medical practice. See P. Alexandre, and Denoyelle, J. (eds.), 'Tweehonderdste verjaardag van de geboorte van Adolphe Quetelet (1796–1874) Stichter van de Sterrenwacht van Brussel', *Astronomisch Bulletin* 1996, Koninklijke Sterrenwacht van België, p. 23.

[10] For a brief history of the use of fingerprint, see also CNIL, *21e rapport d'activité 2000*, Paris, 2001, pp. 103–104.

[11] Ashbourn, Social Implications of Wide Scale Implementation of Biometrics, 2005, p. 5.

[12] Farelo, A History of Fingerprints, 2009, p. 6.

[13] See F. Galton, 'Finger print evidence', *Nature* 1902, p. 606 available at http://galton.org/bib/JournalItem.aspx_action=view_id=291

fingerprint was established. Edward *Henry* was appointed director.[14] He further completed the classification system of Galton, resulting in the Galton-Henry system.[15]

37. The use of fingerprint by police spread from then on fast. By the 1920s, fingerprint identification was used by law enforcement all over the world, including the U.S. military and the FBI, as a form of identification.

2.1.3 Last Decades of the Twentieth Century: Automated Biometric Techniques Develop

38. Since the early twentieth century, hundreds of millions of fingerprints have been collected by police and have been used *manually* for decades. Palm prints were also successfully used in the early 1900s to solve murder cases.

Only in the last decades of the twentieth century, *computer aided* techniques started developing. Hand geometry was used for one of the first fully automated checks against a stored reference.[16]

39. In 1985, the idea that an iris was unique, was promulgated. In 1994, the first iris recognition algorithm was patented, and soon thereafter, a commercial product for the automated measurement of iris became available.[17]

40. Other techniques for the automated measuring of face, speech and fingerprint were proposed and developed, as well as of behavioral characteristics, such as the dynamic signature.[18] Later on, new biometric characteristics, such as vascular patterns, are described and used in recognition systems.

41. At the end of the twentieth century, various large-scale systems deploying biometric characteristics are set up, including in Europe and in the United States.[19]

---

[14] Edward Henry had developed a fingerprint classification system when he was an administrator in Bengal on the Indian subcontinent.

[15] The Henry classification system is still the basis for print recognition in most English speaking countries. Other ten–print classification systems include the Roscher system, developed in Germany and the Vucetich system (see *above* § 34) developed in Argentina.

[16] A U.S. patent was issued to Robert P. Miller in 1971 for the technology that measured the hand characteristics and recorded the unique features for automated comparison and identity verification.

[17] See J. Daugman, 'How Iris Recognition Works', *IEEE Transactions on circuits and systems for video technology*, 2004, pp. 21–30, available at http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf

[18] For an overview, see NSTC, Biometrics History, 2006, 27 p.

[19] For a brief overview of some of these systems, see *below* §§ 142–169.

2.2 The Functioning of a Biometric System

42. The term 'biometric' is based on the Greek nouns 'βίος' (life) and 'μέτρον' (measure) and means 'measurement of living species'.[20] In this book, only biometric methods for the automated measurement of characteristics of human beings is taken into account. We will attempt to give a definition of the term 'biometric data' *below* in Chap. 3 since the term plays a central role in our analysis and research for an appropriate legal framework.

Biometric technologies imply that unique or distinctive human characteristics of a person are *collected*, *measured and stored* for the automated verification of a *claim* made by that person or the identification of that person.

The use of human characteristics for identification purposes is not new.[21] Before the advent of biometric systems, however, human characteristics were compared in a manual way. Biometric systems hence differ from any manual verification method[22] in that the *technology* allows for the *automated comparison* of the human characteristic(s).[23] The systems themselves however *do not identify* individuals. For identification, additional information (for example, information in databases) is needed. Biometric systems only *compare* information submitted. Biometric systems and applications hereby use for such automated process *mathematical* and *statistical* methods for the qualitative and quantitative *measurement* of relevant features which are extractable from human characteristics.

43. In order to study the legal and other issues with regard to biometric systems, it is required to understand the more technical and functional aspects of a biometric system. After a brief discussion of the biometric characteristics fit for use in an

[20] According to the Penguin Concise English Dictionary, biometrics is the 'application of mathematical and statistical methods to the study of biology'. As stated *above*, the Belgian scientist *Quetelet* was one of the first to analyze with mathematical and statistical methods observations in various fields (including astronomy, meteorology and climatology). Applied to humans in the early 1800s, he could be considered as one of the scientists who lay the foundations of modern biometric methods.

[21] For example, police or the military use already since a long time, besides fingerprint, for example, the uniqueness of teeth for identification purposes.

[22] E.g., a border control agent, reviewing a face image on a passport document by comparison with the person in front of him.

[23] Especially the comparison is automated. The presentation and the recording of various human characteristics during enrolment for later comparison remain in principle subject to additional processes and procedures, sometimes under well defined and specific conditions (e.g., after verification of the identity by submitting particular documents or whereby the characteristics are presented by the person in a specific way in order to guarantee good quality data). Cooperation of the person and enrolment is hence in most cases but not always required (see, for each of the characteristics discussed, *below* § 56 *et seq.*). However, the technologies are developing in such a way that also the presentation of the characteristics, e.g. for subsequent comparison, and the enrolment become automated. See, e.g., Iris on the Move, as mentioned *below* in § 60 and the footnote there mentioned.

automated application, an overview of the functionalities of some specific features of a biometric system will be given. This section will conclude with examples of the current use of biometric data in the public and private sector and of standardization efforts in this field.

2.2.1 Biometric Characteristics Used in Biometric Systems

2.2.1.1 The Biometric Characteristics Are Universal, Persistent and Unique

44. Biometric characteristics eligible for use in a biometric system for automated comparison, shall have specific qualities. The mandatory qualities of the characteristics to be used are that the human characteristic shall be universal, persistent and unique or at least distinctive. Some of these characteristics are epigenetic and therefore also unique for identical twins. Epigenetic means broadly that they are developed without genetic specification (without association with the underlying DNA sequence).[24] These specific qualities which render the use of human characteristics fit for biometric systems, will precisely also be at the basis of the risks of biometric systems, as we will argue and demonstrate *below*.

2.2.1.1.1 Universal

45. 'Universal' means that the biometric characteristic shall (in principle) be present with all human beings. The biometric characteristics, which are mentioned *below* are examples of such universal characteristics. The requirement excludes the use of specific traits, such as for example spots, scars or stains on the skin, which may be used to recognize or to identify persons, for example in a disaster scenario, but which are not universal.

46. Even though a biometric characteristic may be considered universal, for example a fingerprint, it does not mean that *all* persons will have the required biometric characteristic. Persons may have lost a biometrically relevant characteristic through accident, sickness or peculiar circumstances. Moreover, some ethnic groups have human characteristics that are less pronounced than average or are different.[25] This means that a biometric system will not work properly in such case[26] and in general that systems will *never* be accessible to *all* persons. This has important consequences, also from an ethical point of view, and should be taken into account in a regulation of biometrics.

---

[24] For example, fingerprint characteristics and iris patterns are epigenetic.

[25] For example, it has been reported that the ridges of the fingerprint of people from Asian countries are less pronounced. See also Chap. 3, footnote 207.

[26] In particular, these groups of persons have a higher risk of false rejections (see *below*).

2.2.1.1.2 Persistent

47. The biometric characteristic also needs to be persistent, *i.e. does not change* over (some) time. Examples of biometric characteristics which meet according to experts this criterion in a convincing way include fingerprint and iris.[27] It is also assumed that a data subject is in principle *not able to change* these characteristics.[28]

48. Some biometric characteristics will be *more susceptible to change than others*. The face of a person, for example, may provide for reliable recognition, but may pose difficulties if used over a longer period because of intended modifications to the appearance, such as by the use of glasses, the growth of a beard or cosmetic surgery, or by unintended changes, such as change by injury, growth (of a younger person), by gaining or losing weight or by ageing (for mid-age to elder persons). The geometry of the hand (and fingers) is another example of a characteristic which may change over time, especially of youngsters. Some therefore prefer to use the term *stability* as a requirement instead of persistence.[29]

49. The criterion of persistence inevitably determines the level of security and reliability provided by the system. It will furthermore have an influence on the usability and effectiveness of a system: in case many individuals are falsely rejected because of unstable characteristics, additional checks will have to be performed and this will lead to long waiting lines. Moreover, costs will increase, as the data subjects will have to be enrolled again at more regular intervals.

The susceptibility of the biometric characteristic to change will also be reflected in errors and should hence be taken into account in the choice of and the decision to implement a biometric application by a particular biometric system. This aspect, however, does not seem to be always taken seriously, even in choices made for large-scale biometric systems. The implications for *reliability*, *cost and trust* are nevertheless significant.[30]

---

[27]This means, as long as there is no evidence to the contrary of the stability. A fingerprint or iris pattern, however, may also be affected over time by illness or damage.

[28]The fact that the data subject is not able to change his or her characteristics, has also important consequences in case biometric data are compromised, e.g., in case of theft. This risk will be further analyzed in Part II.

[29]For the effect of (young) age upon facial recognition, see, for example, X., *2b or not 2b. Evaluatierapport. Biometrieproef. 2b or not 2b*, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2005, pp. 26–27 ('2b or not 2b, 2005'), available at http://nl.scribd.com/doc/21646625/Evaluatierapport-2b-or-Not-2b

[30]London School of Economics and Political Science, *The Identity Project. An assessment of the UK Identity Cards Bill and its implications*, London, LSE. The Department of Information Systems, v. 1.09, 27 June, 2005, p. 12 ('LSE, Identity Project, 2005'), available at http://is2.lse.ac.uk/IDcard/identityreport.pdf The report, which opposed the introduction of the Identity Cards Bill in the United Kingdom, referred in particular to the fact that a considerable percentage of the population is aged, and is likely to fall in the group of people likely to face problems with the use of their biometric characteristics.

2.2.1.1.3 Unique or At Least Distinctive

50. The third criterion for a biometric characteristic to be fit for use in a biometric application, is the uniqueness or at least the distinctiveness of the characteristic. Only biometric features which are *unique or sufficiently distinctive* are fit for recognition purposes[31] by a biometric system. Several biometric systems and applications can be used depending on whether the characteristic deployed is unique or distinctive. This requirement of uniqueness or distinctiveness touches the essence of biometric systems, as the systems are used to identify, to verify the identity or any other claim or to distinguish persons, which is only possible with unique or sufficiently distinctive features extracted from same characteristics.

Uniqueness

51. Fingerprint is generally accepted to be unique.[32] This is also the case for the fingerprint of identical twins which are considered to be sufficiently unique to distinguish one person from the other from the twin couple.[33] The iris, generally considered to be a phenotypic and hence an epigenetic trait, is also unique for identical twins.[34] Even the dynamic characteristics of a handwritten signature are considered unique.

52. While uniqueness is relevant, it remains important to understand that a biometric system *will not verify the uniqueness* of the biometric sample (or template),[35] but the probability that the two submitted samples (or templates) stem from the same person.

---

[31] The recognition purposes, which include both the identification as the verification functionality, are an important aspect of a biometric system. These functionalities will be discussed further *below*. Other biometric characteristics could include length or weight (for example, of a newborn or now also of fetuses by sonographic examinations), but these measurements will in general not be used for recognition purposes.

[32] With regard to the uniqueness of fingerprint, reference is often made to the unpublished statistical '50K' study of the FBI prepared in expectation of litigation to support the uniqueness theory of fingerprints. However, it has been suggested that such accepted uniqueness of fingerprint is more a result of '(i) a striking visual appearance of fingerprints in court, (ii) a few dramatically successful cases, and (iii) a long period in which they were used without a single case being noted where two different individuals exhibited the same pattern'. See B. Weir, *Are DNA Profiles Unique* ? ('Weir, DNA Profiles'), available at http://www.bioforensics.com/conference/Identity/weirindid.pdf who cites and refers in his paper to S. Stigler and his work *Galton and Identification by Fingerprint*, 1995.

[33] See A. Jain, S. Prabhakar and S. Pankanti, 'On the similarity of identical twin fingerprints', *Pattern Recognition*, 35, no. 11, November 2002, pp. 2653–2663.

[34] Monozygotic twins have different iris patterns. J. Daugman, 'Interview. Pattern recognition : Biometrics, Identity and the State – An Interview with John Daugman', in *BioScieties* 2008, p. 82. Some doubt emerges as to the phenotypic character of the iris feature (see Part II, Chap. 4, § 74, referring to recent studies pointing to ethnic information (transferred by genes) in the iris images fit for automated ethnic classification).

[35] See also Weir, DNA Profiles. He states, for example, that there is no satisfactory probabilistic or statistical genetic theory for the growing acceptance of DNA profiles being unique, because of the possible dependencies between loci and between individuals. About the distinction between samples and templates, see *below* §§ 98–101.

This approach is similar as the one taken in *forensic science*. A central question in a criminal investigation is the identification of the suspect (sometimes the victim). For this purpose, samples from a crime scene and from a suspect will be compared. While these samples may be unique, they will not be identical, but they can be used as evidence to demonstrate that the two samples originate from the same source. In case of a categorical statement of identity of source, identification takes place.[36]

Distinctiveness

53. If a biometric characteristic is not unique, it may be sufficient that the characteristic is *distinctive* allowing to separate two individuals. Hand geometry is an example of a characteristic that is used for the distinctiveness rather than the uniqueness of the features.
Distinctiveness is also mainly looked for when biometric methods are used for analyzing behavioral characteristics.

2.2.1.2 Biometric Characteristics Which Meet the Above Criteria

54. Various biometric characteristics are considered to meet the above criteria. A distinction is sometimes made between *biological*, *physiological*[37] and *behavioral* characteristics or traits.

Since 'biological characteristics' is the more comprehensive term (as compared to 'physiological characteristics'), we propose to use the term 'biological characteristics' in order not to exclude any characteristics of the human body.[38]

The most commonly used biometric characteristics are hereunder briefly described. Such characteristics shall be *detectable* and shall allow for the extraction from *repeatable distinguishing features* for the automated comparison and recognition process. These features should ideally have a wide variation between persons

[36] Weir, DNA Profiles, p. 1.

[37] The term 'physiological' refers to physiology ('*fysiologie*'/'*physiologie*'). Physiology is a branch of biology and deals with the *functions* and *vital processes* of living organisms (or their parts (e.g., cells and molecules) and organs), including the human body. Biology (from the Greek words 'βίος' (life) and 'λογος' (reason)) is the science of life, living organisms, *including* their (*physical*) *structure*, function, growth, origin, evolution *and processes*. See also, e.g., W. Boron and E. Boulpaep, Medical Physiology, 2008.

[38] 'Biological characteristics' is also used in the term 37.01.02 of the ISO Vocabulary for Biometrics discussed *below*. On the other hand, the term 'physiological characteristics' is used in the document Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, 11 p. ('WP 29 Working Document on Biometrics 2003 (WP80)') and was retained in a later Opinion 3/2012, both discussed *below*. In this Opinion 3/2012, reference was also made to 'psychological-based techniques', which are in our view however not relevant for biometric systems as we defined *below*.

(sometimes also referred to as 'interclass variation') (for example, iris[39]), while at the same time, when measuring the biometric trait of the same individual, observe a minimum of variation (sometimes also referred to as 'intra-class variation') (for example, face[40]). Other biometric characteristics than those hereunder listed may equally qualify as emerging biometric characteristics used for recognition and comparison purposes, as indicated by further specialized research in the field, and are briefly mentioned as well.

55. Analysis of human DNA is generally still considered *not sufficiently automated* to consider it as a biometric technology.[41] DNA will therefore not be considered or mentioned here as a biometric characteristic used in a biometric system. It will also not fit our suggested working definition of biometric data (see *below*). We will discuss DNA however in Chap. 3, Sect. 3.2 because DNA is used to identify as well, especially in law enforcement. This use of DNA and other related processes have in some areas been regulated already. Because of similarities with biometric data, a comparison is relevant for our analysis of the legal aspects of biometric data processing.

2.2.1.2.1 Widely Used Biological Characteristic

56. The biological characteristics mentioned below are widely used in biometric systems.[42] The biometric properties of these biological characteristics can be derived and measured by automated means. Differences in uniqueness or distinctiveness and of the circumstances in which the characteristics can be captured by the system, will determine the effectiveness of biometric systems, as we will further explain. The choice of one or more particular characteristics for a system will further be influenced by the acceptance of its use by the individuals (see *below* § 76) and may also influence the architecture of biometric systems.

---

[39]Hand geometry, on the contrary, has a low interclass variation (i.e., the hand geometry is for many persons more or less similar).

[40]Face has a considerable intra-class variation for the same person (e.g., by smiling or when growing older). About this aspect, see also J. Pato, L. Millett (eds.), *Biometric Recognition*: *Challenges and Opportunities*, National Research Council, September 2010, p. 3 ('NRC, Biometric Recognition, 2010').

[41]See, e.g., Organization For Economic Co-Operation and Development, *Biometric-based Technologies*, Paris, OECD, DSTI/ICCP/REG(2003)2/FINAL, 30 June 2004 (cancelling and replacing the same document of 28 April 2004) ('OECD, Biometric-based technologies, 2004'), p. 11. See also *below*.

[42]For an overview of the various characteristics which may be used, see also, e.g., OECD, Biometric-based technologies, 2004; European Commission, DG JRC, and the Institute of Prospective Technological Studies, *Biometrics at the Frontiers* : *Assessing the Impact on* Society, Seville, European Commission, January 2005, pp. 31–63 ('JRC, Biometrics at the Frontiers, 2005'); National Science and Technology Council (NSTC), Committee on Technology; Committee on Homeland and National Security, Subcommittee on Biometrics, *Privacy & Biometrics*. *Building a Conceptual Foundation*, 15 September 2006 (updated), 57 p., available at http://www.biometrics.gov/Documents/privacy.pdf (NSTC, Privacy & Biometrics, 2006); NRC, Biometric Recognition, 2010, pp. 31–34.

Fig. 2.1 Facial image taken of visitor for access control purposes and issuance of badge at the European parliament (© E. Kindt. When the facial image was taken, which was mandatory for entering the building as visitor, a specific position was to be adopted. No information was provided to the data subject about the use and purposes of the collection of the facial image, the controller of the processing and access rights)

Facial Image

57. An image of the face can easily be captured, *with or without the cooperation* (and knowledge) of an individual, even from a distance. For purposes of a face recognition system, 2 dimensional (2D) or 3 dimensional (3D) images taken by commercially available or other cameras are used. Infrared illumination is for facial scans sometimes deployed. Images taken by a consumer camera (for example, as embedded in a mobile phone) may also be fit for analysis (Fig. 2.1).

58. The facial image can be analyzed in various ways. The analysis may focus on for example the geometric distinguishing features of the face,[43] the relative distance between and directions of specific points, but also on skin texture. The *distinctiveness* of faces is *limited*.[44]

Fingerprint

59. Fingertips contain ridges and valleys.[45] The ridge-flows form *patterns* such as arches, whorls and loops, three basic patterns recognized and used in the classification systems developed by Vucetich and Henry (see *above* §§ 34–36). Other biometric properties based on patterns are so-called cores and delta's.[46] Specific points known as *minutiae* are used as well. Minutiae are discontinuities in the flow

[43] Feature analysis is widely used in facial recognition technology.

[44] Some technology developed is precisely based on representations of (a limited number of) distinctive characteristics of a facial image. This technology, and the resulting grayscale images, is also referred to as 'eigenface' (meaning: 'one's own face') and is sometimes used as basis for other face recognition technologies. See OECD, Biometric-based technologies, 2004, p. 26.

[45] Ridges are the raised folds of skin on finger(tip)s. Ridges are separated by so-called valleys. Besides fingers, hand palms, toes and the soles of feet also contain ridges.

[46] The core is the center of a particular fingerprint pattern, while the delta is the point where patterns deviate. See also Fig. 2.2.

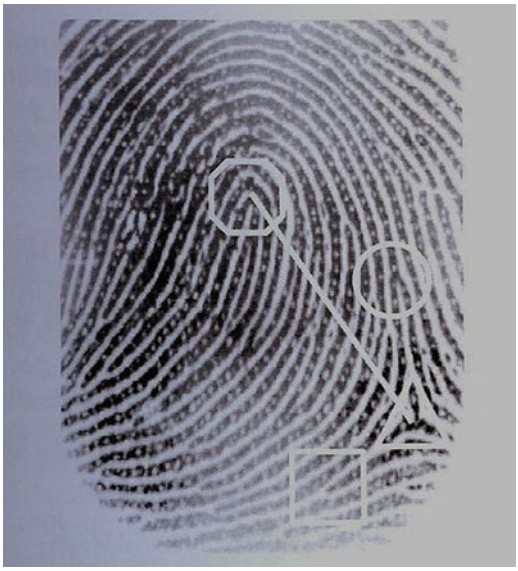

Fig. 2.2 Some biometric properties of fingertips. The core is within the *white octagon*, the *delta* within the *triangle*, the ridge bifurcation within the *circle* and the ridge ending within the *square* (Figure 2.2 is from R. Allen, P. Sankar and S. Prabhakar, 'Fingerprint Identification Technology', (21), p. 33 in J. Wayman, A. Jain, D. Maltoni, D. and S. Maio, (eds), *Biometric systems*: *Technology*, *Design*, *and Performance Evaluation*, New York, Springer, 2005, 370 p)

of the ridges and are mainly the ending or the bifurcation of the ridges. Minutiae and patterns are used in biometric fingerprint systems. Fingerprints, which are the prints left by the ridges of a finger due to secretions of sweat or ink use, are considered *unique*.

Images of the fingerprint are collected by sensors.[47] *Cooperation* of the data subject is in principle needed, but *latent fingerprints*, such as prints left on the sensor or prints found on objects at a crime scene, can also be used, with or without the knowledge of the data subject.

The quality of the image is of high importance. Algorithms, proprietary to the vendor or the system developer(s), are used to reduce the 'noise'[48] of the image and to enhance the ridges. Fingerprint, which has been used in forensic applications for over hundred years, is now widely used in biometric systems in the private sector.

Iris

60. The iris provides rich biometric data in the distinctly *colored ring around the pupil*. The random, *detailed and unique* structure is captured via a sensor to which

[47]The sensors may be optical, using laser light, or be of another type (e.g., using ultrasound).

[48]Noise is a typical term in signal and image processing engineering and refers to (background) elements which are obtrusive for the signal. Noise for fingerprint is for example false minutiae, caused by dirt or by other reasons and other transformations ('distortions').

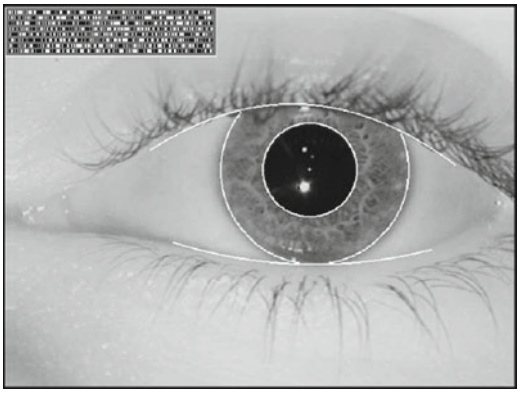

Fig. 2.3 Image of the processing steps for iris recognition: localization of iris boundaries and computation of IrisCode© template (*upper left corner*) (The image is copyrighted and owned by prof. J. Daugman. The image is reproduced with the kind permission of prof. J. Daugman. See also J. Daugman, 'How Iris Recognition Works', *IEEE Transactions on circuits and systems for video technology*, 2004, p. 21, also available at http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf. I also thank prof. J. Daugman for his text suggestions for § 60)

the data subject in principle has to direct his or her eye and which illuminates the iris with near-infrared light. Occluding features such as eyelids, eyelashes, or reflections from glasses, must be detected and excluding from being encoded in the template (Fig. 2.3).

Latest technology, however, permits to capture iris information also at a distance and *without specific cooperation* of the individual.[49]

Hand Geometry

61. The geometry of the hand was one of the first biometric characteristics used for automated verification against a stored reference.[50] The shape and size of the hand palm, finger length, width and thickness of the fingers are measured, as well as curves and the relative locations of these features. In principle, only the geometric features are used for hand geometry and no surface details are recorded, ignoring fingerprints and ridges of the palm, lines, scars and color.

Cooperation of the data subject is in principle required (Fig. 2.4).

[49] See J.R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D.J. LoIacono, S. Mangru, M. Tinker, T.M. Zappia, W.Y Zhao, 'Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments', in *Proceedings of the IEEE*, 2006, pp. 1936–1947, available at http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5%2F4052463%2F04052478.pdf&authDecision=-203 ('Matey et al., Iris on the Move, 2006'). Products are commercially available and include products such as 'Iris on the move'©.

[50] See *above* § 38.

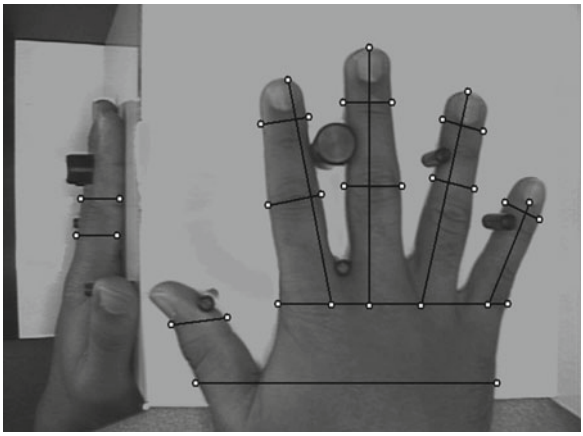

Fig. 2.4 Image of the feature extraction phase of a hand geometry-based verification system (The image is copyrighted and owned by prof. A. Jain, prof. A. Ross and S. Pankanti. The image is reproduced with the kind permission of the copyright owners. See also A. Jain, A. Ross and S. Pankanti, 'A Prototype Hand Geometry-based Verification System', in X., *Proceedings of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication* (*AVBPA*), Washington D.C., 1999, pp. 166–171 ('Jain, Ross, Pankanti, Hand Geometry, 1999'), also available at http://www.csee.wvu.edu/~ross/pubs/RossHand_AVBPA99.pdf)

62. Unlike fingerprint, the *uniqueness* of a human hand is *limited*. The individual hand geometry features therefore do not scale well for identification (in large scale applications) and limits the use of hand geometry to mainly *verification purposes* and small-scale identification applications.[51]

The biometric method based upon this characteristic is vulnerable to *changes* of the hand geometry. Such changes may be caused by for example an injury (e.g., loss of one or more fingers or deformation of the hand), diseases (e.g., arthritis) and aging, but also by wearing jewellery.

Palm Print

63. The print of the palm of one's hand is another unique biometric characteristic fit for use in biometric systems. A palm of the hand has patterns of ridges and valleys, similar to those of fingerprints, as well as lines and wrinkles.[52] While the use of

[51] See Jain, Ross, Pankanti, Hand Geometry, 1999 see also JRC, Biometrics at the Frontiers, 2005, p. 62. This study of 2005 summarizes that the lower part of the hand is less distinctive and that the technology (of that date) measures about 100 points of the hand (e.g., length of fingers, size of knuckles, …).

[52] See National Science and Technology Council (NSTC), *Palm Print Recognition*, 2006, 10 p., available at http://www.biometrics.gov/documents/palmprintrec.pdf

palm print shall be distinguished from the use of the geometry of one's hand as biometric characteristic as explained above, palm print systems may include hand geometry characteristics in their calculations. Because of their uniqueness, palms can be used for identification purposes.

Cooperation of the data subject is in principle required, but not necessary.[53]

Voice

64. One's voice can be used for comparison in biometric systems as well. The characteristic depends on both one's biological and behavioral traits (see about voice also *below*). Both systems based on text spoken by the individual and stored and those having no advance registration of one's speech are used. *Cooperation* of the individual is therefore in principle not required.

Speaker recognition based upon voice can be used for identification[54] (according to some with smaller databases) and verification. While being used until recently mainly in forensic applications, adoption in the private sector has been slow, but increased use may be expected.[55]

Retina

65. The analysis of the retina vascular patterns also provides *unique* characteristics for use in automated identification or verification processes. Retinal scanning analyses the layer of the *blood vessels located at the back of the eyeball* with special lighting. The scan uses infrared or near-infrared illumination and imaging. *Cooperation* is required.

It has been adopted in various military applications because of good levels of accuracy when other biometric techniques were still developing. However, the retina is rather hard to measure and capturing its image requires a great degree of effort and cooperation of the data subjects. The use of the retina has compared with other biometric characteristics declined in popularity.[56] Nowadays, its use is restricted to extremely demanding access control situations, such as in governmental or military settings, for example for access to nuclear weapon or research sites.

[53] In several states of the U.S., statewide palm print databases are in use, allowing law enforcement agencies to submit unidentified latent palm prints to be searched against other in databases of known offenders.

[54] Over 70 (human) body parts participate in creating speech. See Speech Technology Center, *Voice Biometrics. Exciting capabilities of a new biometric modality*, 9.12.2010, presentation at Rise and Hide Conference, Brussels, 9–10.12.2010, slide 2, 4 and 14, available at http://www.riseproject.eu/_fileupload/RISE%20Conference/Presentations/Alexey%20Khitrov.pdf ('Speech Technology Center, Voice biometrics, 2010').

[55] See also Speech Technology Center, Voice biometrics, 2010, slide 11.

[56] Ashbourn, Social Implications of Wide Scale Implementation of Biometrics, 2005, p. 6.

Vein Patterns

66. *Vein patterns* are one of the more recently used characteristic in systems.[57] The structure and patterns of the veins in the hypodermic areas of specific parts of the human body, such as the palm, fingers, back of the hand or the wrist, form a *unique*, clear and constant pattern for each person. Characteristics such as blood vessel branching points, vessel thickness and angles are used.
The vein patterns are captured by high resolution cameras using infrared or near-infrared light. The patterns are then compressed and digitized. The patterns are compared by means of a pattern-matching technique.[58] The system performance is quite accurate. *Cooperation* is needed, but new technology would allow to capture *contactless*[59] in milliseconds images of veins, e.g., of the palm, while *in motion*.

2.2.1.2.2 Behavioral Biometric Characteristics

67. Behavioral characteristics are also used in biometric systems. Behavioral characteristics, such as *typing* or *signature writing* characteristics, are based on behavior which is deemed to be unique or at least *distinctive*, universal and (more or less) persistent. Because the data subject is active, the biometric methods based on these characteristics are sometimes also referred to as 'active biometric methods'. Others however use the term of active biometric methods where cooperation of the subject is needed.

Typing characteristics, in particular the way a person types or pushes on a keyboard, such as the rhythm and error frequency, is *distinctive* and may be analyzed by software. The analysis detects the patterns of the typing and produces a digital measurement, which may be compared to previously stored patterns. This characteristic, also referred to as 'keystroke dynamics', is especially used with passwords, in order to check whether the password was typed by the same person. Although *cooperation* is needed, persons *may not always be aware* when the biometric method is used.

68. The dynamic of someone *writing a signature* is another characteristic used in biometric systems.[60] The way the signature is written with a 'smart pen'

[57] Palm and finger vein authentication are increasingly used, such as for ATM cash dispensers and banking services, for example in Japan.

[58] NSTC, Privacy & Biometrics, 2006, p. 20. The red blood cells (hemoglobin) in the veins absorb the rays and are hence visible on the image as black lines.

[59] See, e.g., Y. Zhou and A. Kumar, 'Contactless palm vein identification using multiple representations', 6 p., presentation and paper at IEEE Fourth International Conference On Biometrics: Theory, Applications and Systems (BTAS) 2010, Washington, U.S.A., 27–29.09.2010 ('BTAS 2010'), 6 p., available at IEEEXplore Digital Library.

[60] See e.g., M. Gasson, M. Meints, and K. Warwick (eds.), *D.3.2*: *A study on PKI and biometrics*, Frankfurt, FIDIS, July 2005, pp. 82–86 ('Gasson, Meints and Warwick, PKI and biometrics, Fidis D.3.2, 2005').

including sensors or on a pad is analyzed by software (e.g., the acceleration, pressure, and the direction of the signature strokes). Signatures have in general always been used as a method of verification, for examples in legal or commercial transactions, and the use of the so-called dynamic signature characteristics is therefore considered as being easily accepted.[61] *Cooperation* is in principle required. The dynamic signature characteristics, however, change over time and are also influenced by the physical and emotional condition of the person (large intra-class variety).

69. *Voice* (see also *above* § 64) can be easily captured with a microphone, *with or without the cooperation* or knowledge of the person concerned. The characteristics are represented by digitized volume images. It is debated whether voice is sufficiently *distinctive* to permit identification from a large scale database of identities. The voice characteristics may also easily be affected by the capture devices, including the communication channel (e.g., the phone), by someone's health (e.g., a cold), emotional state or stress.

2.2.1.2.3 Newly Researched Biometric Characteristics

70. Individuals are presumed to have a distinctive *gait*.[62] Gait, a complicated spatio-temporal biometric characteristic which is further studied and analyzed, promises to be able to do identity verification *from a distance*. This technique and related technologies have been researched but are not yet developed to the same level as other biometric characteristics. Analysis of the *seated posture* is another type of biometric characteristic that has been worked on.

71. The *odor* would also be distinctive from person to person and first steps are made of analyzing the chemical components for use in biometric systems. The shape of the outer flap of the *ear* and the *ear canal* are other biometric characteristics which are researched for use in biometric systems.[63] Other newly researched characteristics for biometric systems include for example fingernail ridgelines.

---

[61] This biometric authentication method was believed to be very promising. See, e.g., the biometric authentication method of LCI-SMARTpen, which promised secure authentication for consumer protection against credit card fraud, home banking en tele-shopping, privacy protection for medical records, etc. and which was the Grand Prize Winner organized by the ESPRIT program of the European Commission of Applied Science and Engineering in 1997. See X., *Convergence* : *Creating the Future Commission*. *President Jacques Santer announces 200,000 ECU European IT Prize Winners*, 25 November 1997, available at http://cordis.europa.eu/esprit/src/eitcp4en.htm

[62] Gait is the way someone walks.

[63] See also, e.g., P. Tuyls, E. Verbitskiy, T. Ignatenko, D. Schobben and T. Akkermans, *Privacy Protected Biometric Templates*: *Acoustic ear identification*, paper submitted at SPIE 2004, available at http://www.sps.ele.tue.nl/members/T.Ignatenko/papers/SPIE2004.pdf

2.2.1.2.4 Other

72. *Brain patterns* and *heart rhythms* are other biometric characteristics which are being researched as new means of biometric recognition. The use of electrocardiograms (ECGs) permit the recording of the heart rhythms while electroencephalograms (EEGs) record the brain's electronic activity patterns. The analysis and use of the physiological response of individuals by a combination of biometric and the latest sensor technologies are still at pre-commercial, proof-of-concept stage.[64]

The use of these physiological characteristics are believed to be promising as they are *internal* processes which offer specific advantages over external characteristics, such as fingerprint, face and voice, which can be faked. They are not prone to leave latent templates (see *below*), can be continuously acquired using minimally intrusive devices and provide intrinsic aliveness detection. They are sometimes also referred to as 'biodynamic indicators'.

73. The expression of *emotions on the face*, which are believed to be universal,[65] may also become subject of further analysis for use in biometric systems.[66] Such emotion-sensing technology allowing 'affective computing' registers human emotions, such as interest, frustration, anger or sadness on faces. This technique of 'face coding' could be used for a wide range of applications, for example in the entertainment industry or for understanding (and influencing) the purchase behavior of individuals. The use of emotions for economic purposes is also referred to as 'emotionomics'.

2.2.1.3 Other Criteria and Required Qualities for Use in Biometric Systems

2.2.1.3.1 Collectability

74. Another mandatory quality of a biometric characteristic for use in a biometric system is the *collectability* of the characteristic. The biometric characteristic must

[64] They are researched, often in combination with other biometric recognition methods (voice, face and gait recognition) by companies and in various projects. See, e.g., the EU-funded project HUman Monitoring and Authentication using Biodynamic Indicators and BehaviOural Analysis (HUMABIO) (2006–2008) (6th Framework programme), at http://cordis.europa.eu/fetch?CALLER=IST_UNIFIED SRCH&ACTION=D&DOC=6&CAT=PROJ&QUERY=011e5a6ef5cd:570d:08b193fe&RCN=78373 and the project ACTIBIO (2008–2011) (7th Framework Programme) mentioned *below* in footnote 75; for research on these and other 'new' biometric characteristics mentioned in §§ 72–73, see also the papers presented and published at BTAS 2010, available via IEEEXplore Digital Library.

[65] See P. Ekman, 'Basic Emotions', in *Handbook of Cognition and Emotion*, Dalgleish, T. and Power, M. (eds.), Sussex, U.K., Wiley & Sons, 1999, 13 p., available at http://www.vhml.org/theses/wijayat/sources/writings/papers/basic_emotions.pdf; see also K. Weintraub, *But How Do You Really Feel*? *Someday the Computer May Know*, 15.10.2012, available at http://www.nytimes.com/2012/10/16/science/affective-programming-grows-in-effort-to-read-faces.html?_r=1&

[66] Images of the human face are studied in detail in order to detect one of the 'basic emotions', such as happiness or fear.

be fit for easy collection and measurement. The collection of iris, for example, is for non-experienced data subjects sometimes problematic because head and eyes need to be positioned correctly.

2.2.1.3.2 Desired Qualities: Usability, Accessibility, Performance and Reliability

75. Additional qualities of biometric characteristics, which are desired include (i) the usability, acceptance and convenience for the person to provide the characteristic, (ii) the accessibility, (iii) the performance, and (iv) the reliability of the characteristic upon the biometric comparison, as explained *below*.

76. An important quality of an biometric characteristic is the *usability* of the biometric characteristic. It refers to interferences that may or may not occur in the use of the characteristic. For example, changes in the face by an accident or illness, as well as changes in its geometry caused by aging, may increase the error rates. Handwritten signatures may be affected by fatigue or the emotional state of the data subject. An aspect of the usability of a biometric characteristic is the acceptance of the technology by the people. *Acceptability* refers to the general agreement with the use of biological characteristics for biometric systems by the public. The use of the facial image or signature, for example, generally benefits from a high(er) level of acceptability, in part also because people are *accustomed* to being recognized by their facial appearance or by their signature.

Biometric systems which *do not require contact*, such as for example facial recognition, seem also to be perceived as less intrusive. Non-intrusive biometric systems benefit generally from a higher acceptance. The use of other characteristics, such as the retina, have low user acceptance because of the intrusiveness of the technology and the fear by some that this may cause injury, such as for retina thermal injury on the back of the eye.[67] The use of fingerprint or of hand geometry sometimes also causes hygienic concerns because of the physical contact with a reader, especially in Asia.[68]

77. Other factors for usability and acceptance are the *user friendliness* of the system and a *speedy matching* decision.[69] Vendors are eager to prove the usability of biometrics in general or of particular biometric characteristics.[70]

---

[67] On the medical aspects, see *below* §§ 139–140.

[68] Gasson, Meints and Warwick, PKI and biometrics, Fidis D.3.2, 2005, p. 82.

[69] Usability and acceptance of biometric systems are aspects which are researched as well, e.g., in the BioSec project (2003–2005) (6th framework program). See, e.g., F. Eschenburg, G. Bente, H. Troitzsch, R. Powierski & O. Fischer, 'The BioSec Mobile Usability Lab for Biometric Security Systems', *Third COST 275 Workshop. Biometrics on the Internet*, 27–28.10.2005, University of Hertfordshire, United Kingdom, pp. 67–70.

[70] See, e.g., Unisys, *Research Shows Growing Global Acceptance of Biometrics among Consumers for Protecting Identities and Personal Information*, 10.11.2009, available at http://www.unisys.com/unisys/news/detail.jsp?id=1120000970000610143

Specific cultural or religious concerns, however, may pose problems for the use and the acceptability of specific characteristics, such as of the face, sometimes covered in whole or in part, of for example Muslim women or Sikhs.[71] This type of concerns affects the acceptability and also relates to ethical aspects will be further discussed in Part II, Chap. 4, Sect. 4.4.

78. *Accessibility* refers to the way the biometric characteristic and the corresponding technology can be used and whether data subjects can easily enroll. Each characteristic and related technology may have its own difficulties. For face recognition, for example, the sensors will have to be adjustable, in order not to cause difficulties for either tall or short data subjects or data subjects in wheel chairs. Speech and hearing impaired data subjects may be unable to use voice recognition systems. The accessibility may also imply ethical concerns, which we will discuss *below*.

79. Since the biometric comparison is a technological process in which signals are captured and compared, the *performance* of the measurement process of the biometric characteristic shall not only be robust and fast, but also accurate and efficient. Many biometric methods and systems do not meet these qualities and the performance of many systems could still be (much) improved. The description of the functional characteristics of a biometric system *below* will explain the elements which affect the performance of systems (e.g., the functionality used) and how various parameters can be set and adapted (e.g., the desired error rates) to influence the system performance. These elements and parameters are often not known to a wide audience.

80. The *reliability* refers to the quality that the biometric characteristic is not easy to forge and that the delivery of the characteristic is not apt to fooling the system. Some characteristics (for example, fingerprint) are more apt to be copied than others. Several examples will be discussed in Part II, Chap. 4 on the risks of biometric data processing. If the system can be easily circumvented, the delivery of the characteristic to (non attended) systems is in that case problematic.[72] Systems are sometimes equipped with liveness test features to tackle this problem, but liveness detection is not always easy or effective.[73]

---

[71] Sikhs, for example, are required to wear the 'dastaar' (turban) at all times.

[72] See, for example, about a South Korean woman, barred from entering Japan, who reportedly passed through an immigration biometric control by using tape on her fingers (and a false passport) to fool the fingerprint reader. See X., 'Woman fools Japan's airport security fingerprint system', *the Sydney Morning Herald*, 2.01.2009, available at http://www.smh.com.au/travel/woman-fools-japans-airport-security-fingerprint-system-20090102-78rv.html. In another case, also widely in the news, however, a Chinese woman had plastic surgery done to alter her fingerprints to fool immigration controls for entering Japan. See 'Fake fingerprint' Chinese woman fools Japan controls', BBC Worldnews, 7.12.2009, available at http://news.bbc.co.uk/2/hi/asia-pacific/8400222.stm. On this (ethical) issue, see also *below*.

[73] About liveness detection techniques for fingerprint and their effectiveness, see, e.g., D. Maltoni, D. Maio, A. Jain and S. Prabhakar, *Handbook of Fingerprint Recognition*, London, Springer, 2009, pp. 386–391, in particular no 9.5.2 ('Maltoni, Maio, Jain and Prabhakar, Handbook Fingerprint, 2009'); see also Part II, Chap. 4, § 103 and footnotes.

2.2.1.3.3 Other

81. The above criteria will be further completed for practical applications. Criteria such as how resistant the characteristic is against use by *impostors* or (*identity*) *fraud* and the *interoperability* of systems are hence also important aspects. They relate to the risks of the use of biometric characteristics, and will be further discussed in Part II.

2.2.1.4 Soft Biometric Characteristics

82. Soft 'biometric characteristics'[74] would in principle not meet the criteria above, in particular the criteria of uniqueness and persistence. Examples of soft biometric characteristics are height, weight or fat percentage.

83. Nevertheless, soft 'biometric characteristics' are increasingly used. They are in many cases deployed in combination with other biometric characteristics, such as fingerprint, to *improve the performance* of the system.[75] These biometric characteristics may also be used to enrich the *profile* of individuals. An exact definition of soft biometric characteristics has been proposed nor is generally accepted yet.[76]

2.2.1.5 Other Physical Characteristics

84. Human beings may have various other characteristics of a physical nature which can identify or distinguish them from others. Scars, marks or tattoos, for example, allow to identify persons, for example in criminal investigations. These

[74] Since the characteristics can not be used to distinguish or to identify, the term biometric characteristic is in fact not appropriate; see also, about the biometric vocabulary, *below* §§ 96–97.

[75] See, for example, H. Ailisto, E. Vildjiounaite, M. Lindholm, S. Mäkelä and J. Peltola, 'Soft biometrics-combining body weight and fat measurements with fingerprint biometrics', *Pattern Recognition Letters* 2006, pp. 325–334; for recent research using soft biometrics, see also the presentations and papers presented at BTAS 2010; for research on soft biometric characteristics in combination with gait, see the EU-funded project ACTIBIO (2008–2011), with website at www.actibio.eu

[76] See the description in the Opinion 3/2012 of the Article 29 Working Party (see *below*) as 'the use of very common traits not suitable to clearly distinguish or identify an individual but that allow enhancing the performance of other identification systems' (p. 16); about the need for a (legal) definition and the use of soft biometric characteristics in profiling applications, see E. Kindt, 'Need for Legal Analysis of Biometric Profiling', Reply to V. Andronikou, A. Yannopoulos, Th. Varvarigou, 'Chapter 7. Biometric Profiling : Opportunities and Risks', in M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, 2008, (139), p. 142 ('Kindt, Need for Legal Analysis of Biometric Profiling. Reply, in Hildebrandt and Gutwirth, Profiling the European Citizen, 2008').

characteristics are in some cases removable or can easily be manipulated. Because these traits are *universal nor persistent*, they are in general not recognized as biometric characteristics for use in automated claim or identity verification or identification applications.[77,78]

2.2.2 Use of Biometric Characteristics and Functionalities of a Biometric System

2.2.2.1 Identification Versus Verification

85. As mentioned, biometric technologies collect and usually store unique or distinctive biological and/or behavioral characteristics of a person for the automated *verification* of a(n identity) claim or for the *identification* of that person. This description mentions the two main functionalities of biometric systems: identification and verification.[79] These two functionalities (or modes) are very different and *a distinction between those two functionalities* is crucial and of major importance for understanding biometric systems and for the discussion about the use of biometric data.

86. First of all, the *purpose* (*i.e.,* the manner or the specific way the comparison is done[80]) of the (identity) verification function as opposed to the identification function is different.

The *verification function* compares the submitted biometric characteristic *with one particular* biometric characteristic. This characteristic is usually *previously submitted and already stored*. Verification is therefore also referred to as a 'one to one comparison' (1:1 comparison). It gives an answer on whether both characteristics *belong to the same person*. If the 1:1 comparison result is positive, the system

[77] This may however change. See the research project on '*Automatic* Matching and Retrieval of Scars, Marks and Tattoos' (stress added) of Anil K. Jain and Rong Jin at Michigan State University for assisting law enforcement agencies in identifying suspects and victims and which received funding from the FBI, announced at http://www.cse.msu.edu/~rongjin/r_project_tattoo.html

[78] About this type of characteristics and our proposed definition, see also Chap. 3, §§ 271–282.

[79] A (legal) definition of biometric systems hardly exists. The Article 29 Working Party (see *below*) has described biometric systems in 2003 in similar terms, as 'applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person'. It repeated this description in its Opinion 3/2012 (see *below*) while proposing 'a more general definition' for biometric systems as 'a system that extracts and further processes biometric data' (p. 5). For our proposed definition of biometric data, see Chap. 3, §§ 272–282. See also the recent Protection of Freedoms Act 2012, referenced in Chap. 3 footnote 509, and its definition in Chap. 2, § 28 (4).

[80] The purpose is here understood in the strict sense, *i.e.,* the way the comparison is done. This is as opposed to the meaning of 'purpose' in the data protection legislation, i.e., the purpose of the use of the data.

will render a positive comparison decision, as a result whereof, for example, the person can enter the place or log into the network.

The *identification function* recognizes an individual by comparing the submitted biometric characteristic *with all previously submitted and stored biometric characteristic in one or more database*(*s*) through a search. This is also referred to as a 'one to many comparison' (1:n comparison). If a comparison is made with only a limited number of earlier submitted characteristics, the term 'one to few' comparison is sometimes used. This comparison nevertheless remains an identification. The identification functionality tells upon comparison *if the biometric characteristic*(*s*) *has* (*have*) *already been previously stored* as a reference and is present in the biometric reference database(s) or not. If it is the case, it allows to tell (i) *whether* the data subject is registered (or not), and/or (ii) if names or other personal details are mentioned with the stored characteristics in that database (or which can be linked to these characteristics), *to whom the submitted biometric characteristic belongs*. It is clear that the system can only provide trustworthy information about the identity of the person to whom the characteristic(s) belong if and only if upon the enrolment of the characteristic(s) (and registration) the link between that person and the identity he or she claims has been carefully reviewed (for example on the basis of reliable documents). Another aspect is that for the identification functionality, databases belonging to third parties could in principle be used as well – especially if samples of the characteristics are stored – in order to compare and to obtain information about a given person.

The identification functionality is interesting. First of all, it allows to check whether or not *someone is on a particular list* or database. This list may also be a so-called 'watch list' or a black list.[81] The functionality further allows to tell whether someone *has been registered before*, referred to as a so-called double enrolment check ('DEC'). This can be useful to know or to review, for example, when someone exercises a right or an entitlement twice (e.g., a voting right, a right to a social benefit or an asylum application) (also called 'double-dipping'), or when there is an interest to avoid that someone is listed twice (e.g., it is prohibited that someone obtains a document twice (e.g., a passport (the second time) under a false name)). The use of biometric characteristics excludes in this case that false names can be used. Last but not least, the identification functionality can be used by the controller to *identify* persons.

87. It should be clear from the above that a biometric system executes the two functionalities in a substantially different way: (1) verification is possible with a (mere) comparison of one submitted set of characteristics with a pre-defined and pre-stored

[81] The way the identification function is used hence does not necessarily provide identity information, but merely a so-called 'hit', i.e. a confirmation that the person is on the list. A person who is not on the (watch or black) list, will therefore not necessarily be identified by the biometric search.

set of characteristics, while (2) identification compares the submitted biometric characteristic with many, in principle the whole set of the previously stored biometric characteristics (in the database(s)).[82]

88. Secondly, the *architecture* will in principle also be *different*. The identification functionality will always need the existence of a *database* with the biometric data stored for comparison. The verification functionality only requires the storage of one specific set of the biometric characteristics, with which the 'fresh' biometric data[83] will be compared. Such storage can be done centrally, for example in a central database, but it is also possible to store the biometric data for comparison locally, for example on an object which the data subject holds and which remains in his or her possession.

Verification and identification functionalities, however, may sometimes also be combined in one system. In that case, the architecture will facilitate both functionalities, as both local storage and database are provided for.

89. Thirdly, the *performance* and the *accuracy* of the system for both functionalities is different. The comparison with designated biometric data (verification) is technically less challenging than the comparison with hundreds, thousands or millions of biometric data references stored in a database (identification). One of the problems is that in the latter case, the interclass variability diminishes because of the high number of data subjects, leading to an overlap in the representations of the characteristics of different subjects and hence to reduced results of the comparison system. The accuracy performance for both functionalities is therefore substantially different.[84] Moreover, *even if* the error rates for the verification as compared

---

[82] A distinction is also made between an 'open-set identification' and a 'closed-set identification'. In the former case, the identification functionality (1:n comparison) is used to see whether the person is registered (mentioned) *or not* on the list as we explained *above*. This – upon the hypothesis that one is claiming that he or she is not registered (e.g., to obtain a social security benefit) – actually refers to a negative identity claim, but is sometimes referred to as 'negative identification'. In SD2 Version 12 – Harmonized Biometric Vocabulary (see term 3.5.8), it was then stated that this term was depreciated; but see *below* footnote 91. On the importance for the biometric comparison process, see also Maltoni, Maio, Jain and Prabhakar, Handbook Fingerprint, 2009, pp. 14–15, no 1.5.5.

[83] 'Fresh' biometric data refer to the submitted biometric characteristic(s) and the data extracted at every next occasion of submission for later comparison.

[84] On this issue of 'overlap', see also L. Müller, '3.1.2 Reference model of a biometric system' in E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 26–27 ('Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007'). More precisely and technically speaking, the ability to separate for example different reference templates (see *below*) diminishes in proportion with the density of reference template vectors in the feature vector space. A high density leads to an overlap of the acceptance range around the different reference template vectors of the data subjects and thus to ambiguous results of the comparison system. Performance and accuracy is hence very much related to the density of the points in the feature vector space. If the density remains sufficiently low (such as for iris), the identification can have good results with a very high number of data subjects. The performance variations for verification and identification will be explained *below*.

with the identification functionality would be similar, the use of databases for the identification functionality would imply that even with 1 or 2 % of false rejections or false acceptances on millions of records, a high number of individuals will permanently incorrectly be rejected or accepted. Accuracy is also affected, as a high number of records in a database also implies a high number of possibly *false or incorrect records*. In order to improve performance, *new protocols* have been developed, for example for a combination of both functionalities.[85]

90. Last, but most importantly, the implications for *the risks and the fundamental rights* of the data subject upon the use of their biometric data for *identification* as compared to *verification* is very different and is hence closely connected with the *functionality* used. Because of the place of storage of biometric data needed for verification, biometric data processing for verification has the potential to be more 'controllable' from the point of view of the data subject involved. This will be further explained and analyzed in detail *below*.

2.2.2.2 Authentication of Claims

91. In general, biometric applications are mostly referred to as systems which allow to *authenticate claims*. The verb 'to authenticate' can be described as 'making authentic, legally valid'. 'Authentic' has several meanings, including '1. written or made by own handwriting, not falsified, (…) real, originating in reality from whom it is attributed, 2. corresponding with the original and therefore authoritative (…) 5. of which the reliability is guaranteed (…) 6. carrying an own characteristic (…).[86] The meaning of 'authentication' is understood by us in the broadest way, *i.e.,* guaranteeing the reliability. For example, for individuals entitled to *claim access* to a specific place, a service or a system, biometric systems offer now means to enhance the security and to ensure the reliability, *i.e.* authentication, of their claims. The place may be restricted to named persons or to persons who have specific rights.[87]

---

[85] For example, with so called 'few-to-many' systems, first a list is made based upon identification after a comparison with the database with potential candidates for a successful comparison, where after the verification functionality is applied. About such type of system, see, e.g., J. Bringer, H. Chabanne, T. Kevenaar and B. Kindarji, 'Extending match-on-card to local biometric identification', in J. Fierrez, J. Ortega-Garcia, A. Esposito, A. Drygajlo and M. Faundez-Zanuy (eds.), *BioID_MultiComm'09 Proceedings of the 2009 joint COST 2101 and 2102 international conference on Biometric ID management and multimodal communication*, pp. 178–186. About the further clouding of the 'verification/identification' dichotomy, see also Wayman, Jain, Maltoni, Maio, Biometric systems, 2005, p. 7. We do not agree with the authors however that this distinction would for this reason not be of any further use.

[86] Van Dale, general dictionary of the Dutch language, 13th edition (1999), at the terms '*authentiseren*' and '*authentiek*'. The term 'authentication' ('*authenticatie*') in Dutch is therein not mentioned, but has been added in the 14th edition (2005). In this edition of 2005, the meaning of 'to authenticate' is now completed with 'to establish the identity of'.

[87] This place can be a club, a place at work, a public area and even a country. Similarly, it could also involve access to a system or infrastructure.

Traditionally, an individual who attempts to gain access is authenticated by a (user) name or number, a password and/or personal identification number (PIN), i.e. something that he or she *knows*.[88]

These *knowledge-based authentication methods*, however, do not in all circumstances offer the required security: the information can be easily shared, forgotten or stolen and the methods relying on such knowledge of information are therefore not foolproof. Therefore, a second authentication factor is sometimes added to increase the security. This factor would in particular be something that the individual has in his or her *possession*, i.e., a special document (e.g., an identity card), a token or a card (badge), which are needed to access the restricted place.

Because each of these methods have their draw backs (e.g., high cost of password maintenance, denial of access in case of loss, ….), even if they are combined, biometric characteristics are used as a *third factor* for authentication. Biometric data are hereby deployed to authenticate claims in case or because the two fore mentioned methods are (deemed to be) not sufficient from a *security* point of view, or because of *convenience* reasons (an individual always carries his biometric characteristics, they cannot be forgotten, are easy to use, ….).

92. The biometric data will hereby be used to authenticate a claim that the individual makes. This claim is in the first place a *biometric claim*. A biometric claim is that the data subject is (or is not) the *bodily source* of biometric reference data. For a verification system, this claim could for example be as follows: 'It is claimed that the fingerprint template stored on this token comes from the body of the *same person* submitting the fresh sample and therefore that this person is entitled to enter'. Although the claim is already supported by the fact that the person is holding the card, security is enhanced by the use of the biometric characteristics which allow in addition to verify that the right person is holding the right card.

The claim, however, could more generally be *any claim*. A biometric system can be used to authenticate not only a biometric claim, but also an *identity claim*. For example, 'this person claims to be Bob. A (biometric) identity card has been issued to Bob in person (after review of his identity credentials (for example, birth certificate) from which it appears that he is indeed Bob) and the identity of the holder of this card is verified by the biometric system' (identity claim).

The claim could also be a *rights claim* or an *authorization claim*, and can be combined with one another or with an identity claim. For example, 'Bob claims that he is (Bob and) an employee of this company, is entitled to hold and use his (biometric) employee card (which will need a review of his employment contract) and that he (is Bob and) has the right to enter the premises of the company, restricted to rightful holders of (biometric) employee cards' ((identity and) rights claim). An *authorization claim* refers to a (legal) *mandate*, for example a claim of an individual that he or she is mandated and entitled to represent someone or some entity, or to an

[88] Additional information which the individual alone is presumed to know, could be asked, such as favorite color, which could be stored for later comparison with the information given by the data subject who needs to authenticate him or herself.

authorization, for example that he or she is entitled to enter places. For example, 'Alice claims that she (is an employee and) holds this particular function in the company and is therefore mandated to sign this transaction/ is therefore authorized to enter these specific (high security) premises or applications of the company' ((rights and) authorization claim).

93. In the examples mentioned *above*, the biometric characteristics could be used to ascertain that the person exercising the claim and the associated right(s) is either on the *list* of the *named* individuals (use of the identification functionality) or that it is the *same* employee as the one who has been previously registered as being entitled to enter (use of the identification or verification functionality). It is hence important *to determine which claim is made* and *needs authentication* in order to be able *to specify which particular use of the biometric data is required*. In other words, each particular claim allows for a different use and functionality of the biometric system, requiring in addition other enrolment credentials.

The biometric data can also be used to check whether a person *belongs to a particular group*, often in combination with an identity, rights or authorization claim. An example of such claim is: 'I am a member of this sports club and am entitled to have access to the sports facilities reserved for members only' or 'I am a pharmacist (and belong to the group of pharmacists) and I am entitled to access (anonymously) particular online resources'. For this purpose, *i*t is also not required to *reveal* upon comparison *the identity of the individual* and the *biometric data do not necessarily need to be revealed*.[89]

94. Furthermore, a biometric claim may be *positive*, which means a claim that the data subject *is enrolled* in the system, but a claim may also be *negative*, which means a claim that the data subject is *not* enrolled.[90] Both kind of claims are used in biometric systems. A positive claim, for example, will check whether someone is on the list and therefore authorized to access. A negative claim, for example, would check if someone is not on a list, for example a so-called 'watch-list'. The claim could also be *specific*, i.e. that the specific data subject is or is not enrolled as a *specified* biometric enrollee. The claim, however, could also be *non-specific*, i.e., that the specific data subject is or is not amongst the group of enrollees.[91]

95. From the above, it becomes clear that biometric systems should in most cases be seen as *part* of a larger *identity management system*. The meaning of an identity management system (IdM system), the interests involved, the purposes of the processing and the role of biometric data in such system will be further elaborated in Part III.

---

[89] This type of claim will be further reviewed in Part III, Chap. 7, §§ 105–106.

[90] See term 37.06.04 Note 3 of the ISO Vocabulary for Biometrics 2012 mentioned *below*.

[91] A positive biometric claim is then the assertion that the data subject *is* the source of a specified (e.g., by the use of a PIN) or unspecified biometric reference(s) in a biometric reference database, while a negative biometric claim is the assertion that the data subject *is not* the source of a specified or unspecified biometric reference(s) in a biometric reference database. See the terms 37.06.17 and 37.06.14 of the ISO Vocabulary for Biometrics 2012 mentioned in footnote 94 *below*.

2.2.2.3 Terminology

96. Biometric systems and applications vary very much and the architecture and design are from time to time *complex*. There may be numerous components of a biometric system and a starting point for a discussion about biometric data processing in general should be an agreement about the content, the meaning and the functionalities of the biometric terms used. We have stressed before the importance of clear definitions and of an agreement on the understanding of the terms used in the debate about biometric data processing.[92]

97. Working Group 1 of the Subcommittee 37 of ISO/JTC 1[93] has invested many efforts in the establishment of a harmonized vocabulary and adopted a standard in 2012 ('ISO Vocabulary for Biometrics 2012').[94] Various terms, which were initially deployed in the sector, have become depreciated. It is recommended, for example, to no longer use the general term authentication for the functioning of a biometric systems.[95] This term is not precise on the issue of *which* functionality is used. It is hence preferred to deploy either the term identification or verification. We fully concur that the term 'authentication' is confusing. It will become clear from our further legal research that *distinguishing the use of the two functionalities of biometric verification and biometric identification is crucial*. In addition, maintaining consistent terminology, especially in a debate over various aspects of a complex technology, which requires often an interdisciplinary approach, is necessary for a fruitful discussion about the legal aspects of biometric systems.

We will therefore attempt to adhere in this work as much as possible to the terms of the ISO Vocabulary for Biometrics 2012.[96]

---

[92] E. Kindt, 'Biometric applications and the data protection legislation. The legal review and the proportionality test', *Datenschutz und Datensicherheit* (DuD) 2007, (166), p. 167 ('Kindt, Biometric applications and the data protection legislation. Review and the proportionality test, 2007').

[93] See *below* § 175.

[94] ISO/IEC 2382–37:2012 Information technology – Vocabulary – Part 37: Biometrics, 13.12.2012, 28 p. ('ISO Vocabulary for Biometrics 2012'). Discussions about terminology will refer to this ISO Vocabulary for Biometrics 2012. A translation of the terms in French and German subject to national approval can be found at Ch. Bush, *Vocabulary*, available at http://www.christoph-busch.de/standards.html. Because the terms for a harmonized biometric vocabulary were during our research not yet adopted, we used initially also a draft version of the ISO standard: ISO/IEC JTC 1/SC 37, *Standing Document 2 – Harmonized Biometric Vocabulary*, version 12, N 3385, New York, ANSI, 16 September 2009, working draft text, 203 p. ('SD2 Version 12 – Harmonized Biometric Vocabulary'), to which we may refer from time to time as well. In this draft document, various schemes were also used, for example to reflect the process flow.

[95] See term 37.08.01 ISO Vocabulary for Biometrics 2012.

[96] For another oversight of terms and frequently asked questions on biometric systems, which used the (draft) ISO Vocabulary, see e.g., the site Bioidentification, available at http://www.bromba.com/faq/biofaqe.htm

2.2.2.4 The Phases of a Biometric System

2.2.2.4.1 Enrolment

98. The enrolment[97] is in most cases the first step of a biometric comparison process. During enrolment, a biological or behavioral trait is *delivered* (i.e., submitted by the data subject) and subsequently *captured*[98] via a suitable capture device (for example, a fingerprint sensor). Usually, other information about the individual is also collected and registered. The result of the capture is *the captured biometric sample*,[99] which is the captured 'analog or digital representation of biometric characteristics prior to biometric feature extraction'.[100] We will refer to captured biometric samples herein as 'samples'. It can be decided that the biometric system will use only samples for storage and later comparison.[101]

99. However, in many other cases, so-called templates will be used. A combination of both is also possible and both sample and template would in that case be stored during enrolment. This stored information is designated in a biometric system as respectively the 'reference sample(s)' and the 'reference template(s)'. The choice to use either samples or templates in a biometric system has important consequences for the fundamental rights of the data subjects, as will be explained in Part II.

100. If a template is created, two further processing steps take place. First, there is some pre-processing which enhances the quality and transforms the sample in a suitable way for the next feature extraction step.

Thereafter, the *feature extraction* step uses algorithms[102] for the determination, the preservation and the extraction of the distinct and repeatable *biometric features* (e.g., the minutiae points from a fingerprint or the various patterns) from the sample.[103] The feature extraction and their use aim to facilitate the comparison.

---

[97] The enrolment is sometimes also referred to as the registration process.

[98] Capture refers to the recording and the evaluation of the signal by the system, in particular by the capture device. The result is a sample. A system policy will decide when the capture is sufficient.

[99] The captured biometric trait may be subject to processes that enhance the quality of the acquired sample. Such processes could include, for example, using a number of acquisitions to produce the sample.

[100] See the terms 37.03.21 and 37.03.25 of the ISO Vocabulary for Biometrics 2012. Some refer to the captured biometric samples as to 'raw biometric samples' or to 'raw biometric data', as compared to templates. These terms are according to the ISO Vocabulary for Biometrics 2012 however depreciated.

[101] For example, for the ePassport (see Part III). Biometric systems used for law enforcement purposes presently most often deploy samples.

[102] For the meaning of algorithm, see § 110.

[103] This step is critical from a security evaluation point of view, because the level of uniqueness inherent in a template will influence the FMR (see *below*). See Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Biometrics in identity management, Fidis, D.3.10, 2007, p. 21. See also in particular Fig. 2.5 illustrating some of the processing steps for a fingerprint recognition system.

```
1
2  33 Minutiae Detected
3
4      0 :   18,   84 : 13 :  0.12 :BIF
5      1 :   22,   41 : 16 :  0.13 :RIG
6      2 :   25,  127 : 26 :  0.28 :BIF
7      3 :   27,   67 : 29 :  0.58 :RIG
8      4 :   39,   26 : 17 :  0.12 :RIG
9      5 :   45,  157 : 25 :  0.12 :BIF
10     6 :   52,   40 : 16 :  0.29 :RIG
11     7 :   54,   28 :  2 :  0.29 :RIG
12     8 :   55,   63 : 29 :  0.30 :RIG
13     9 :   61,   80 : 27 :  0.30 :RIG
14    10 :   65,  177 : 23 :  0.12 :BIF
15    11 :   78,   41 : 14 :  0.13 :RIG
16    12 :   80,   73 : 25 :  0.29 :RIG
17    13 :   82,   37 : 11 :  0.29 :BIF
18    14 :   82,  102 : 23 :  0.29 :BIF
19    15 :   83,   65 : 29 :  0.12 :BIF
20    16 :   83,   76 : 26 :  0.29 :BIF
21    17 :  105,  152 : 21 :  0.62 :RIG
22    18 :  107,   25 : 28 :  0.31 :RIG
23    19 :  110,   83 : 19 :  0.29 :RIG
24    20 :  110,  108 : 20 :  0.29 :RIG
25    21 :  113,   41 : 14 :  0.58 :BIF
26    22 :  132,  161 : 20 :  0.60 :BIF
27    23 :  136,  104 : 18 :  0.59 :RIG
28    24 :  145,  168 :  4 :  0.60 :RIG
29    25 :  156,   71 : 16 :  0.59 :BIF
30    26 :  171,  160 : 19 :  0.57 :RIG
31    27 :  173,  184 : 19 :  0.12 :RIG
32    28 :  175,  210 :  4 :  0.06 :RIG
33    29 :  175,  212 :  4 :  0.06 :BIF
34    30 :  214,   98 : 16 :  0.58 :BIF
35    31 :  249,   77 :  0 :  0.59 :BIF
36    32 :  273,  179 :  1 :  0.06 :RIG
37
```

Fig. 2.5 Illustration of one of the feature extraction steps of a fingerprint biometric system (*left*) and of the biometric reference template (*right*) (Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, p. 23. The illustration is reproduced with the kind permission of dr. L. Müller)

These extracted biometric features, which could consist of one or more sets, are then used for the creation of the template. A *biometric template* is the 'reference biometric feature set'[104] which will be stored and then used for later comparisons.

A template may include additional information about the format and encryption of the biometric and other data.[105] The figure *above* also illustrates the typical data reduction from the sample to the template.

Templates, however, being extracted reference biometric features, take *different forms and formats* (or representations). Templates may be, for example, a table or a (fixed-length) numerical (binary) string (e.g., 101010 representing a feature vector[106] or not), differing in details and length. The templates will also vary for each of the characteristics. For example, for fingerprint, the minutiae features may be represented as an unordered set of tuples consisting of the minutiae's coordinates and local orientation. For hand geometry, the geometrical properties of the hand are represented by a fixed-length ordered vector of the lengths and widths of the fingers

[104] Term 37.03.22 ISO Vocabulary for Biometrics 2012.

[105] These templates may be represented in a standardized format (e.g., the BioAPI standard for the format, including the metadata for interoperability, called Biometric Identification Record (BIR), as defined).

[106] A feature vector is a (multi-dimensional) vector (*i.e.* a sequence of elements) of features for representing a characteristic.

and/or palm. Iris are represented as fixed-length binary strings.[107] A biometric sample can also be processed in several successive templates.[108]

101. The size in bits and bytes of a template is typically much smaller than the size of the image. The reduced amount of (kilo)bytes facilitates the storage of templates in for example micro-processors (i.e., chips) which have a limited storage (and processing) capacity and which may be incorporated in smart cards[109] or documents. Depending on the biological or behavioral characteristics and algorithms used, the amount of bits of the template will vary, and may restrict the possibility for particular biometric characteristics to store the information on a card or token.

102. The enrolment hence typically provides the biometric sample and/or the reference template of the biometric characteristic which will be used for later comparisons. This reference can be *stored* in a centralized way, for example, in a database, or on a local object, for example on a portable token held by the data subject.

At the same time, *biometric systems do not always require previous enrolment*. For some biometric systems, the controller will only want to check that someone has not been previously registered (for example, for watch lists, as someone who disturbed the order at a previous incident or is on a list of searched persons (of the police) (negative identity claim)).[110] In this case, most data subjects will not be previously enrolled or registered by the controller. The controller, however, could make use of the enrolment or registration (databases) of other controllers in case the intention would be to identify the persons who were not previously enrolled (risk of linking across databases, further discussed in Part II, Chap. 4).

103. Because of the natural evolution[111] of the biometric characteristic (e.g., for face), accidents[112] (e.g., for finger(print) and hand) or disease (e.g., for iris), it may be required for a given biometric system to re-enroll from time to time.[113]

---

[107] For iris, see the template in the upper left corner of Fig. 2.3 *above*. The binary strings are often displayed as an image with black and white blocks, which is a visualization of the binary string.

[108] For fingerprint, the minutiae could e.g., be represented by spectral minutiae, and thereafter by fixed length vectors. For a (technical) doctoral thesis on this subject, see H. Xu, *Spectral Minutiae Representations for Fingerprint Recognition*, Enschede, Gildeprint, 2010, 174 p. ('Xu, Spectral Minutiae Representations, 2010').

[109] A smart card is a credit-card-size token, but could also be smaller (e.g., a SIM card) and embeds integrated circuits. Such card is also referred to as chip card or integrated circuit card. A smart card contains memory (storage) capacity (such as magnetic-stripe cards do as well) and a processor. International standards exist (e.g., ISO 7810/16). Smart cards are fit to serve a large variety of purposes, not only financial transactions purposes, but also identification (e.g., if combined with a public key infrastructure).

[110] See, for example, the use of biometric face recognition in Tampa, Florida during SuperBowl (see Chap. 3, § 297).

[111] For example, aging.

[112] For example, injury.

[113] This should be one of the requirements of e.g., an identity scheme operated by the government.

2.2.2.4.2 Comparison

104. During this step, the biometric data extracted from the submitted biometric sample (query sample) is compared with the reference sample or the template. It takes usually place after previous enrolment of the data subject, but as stated *above* enrolment is not always necessary.[114] As stated *above*, this comparison may be against a single sample or template (verification functionality) or against a database of samples or templates (identification functionality).

The elements which shall be taken into account for the comparison are in general not fixed. Suppliers of biometric systems will decide through means of extraction algorithms which information will be used for the comparison by their comparison algorithms. For fingerprint data, for example, the minutiae, the patterns or the image, or a combination thereof, can be used for the comparison.[115]

105. For the comparison process, a major issue is the relation between the interclass and intraclass variability of biometric characteristics (see *above* § 54 and § 89): persons can only be recognized in a reliable manner if the variability among different captures of the characteristic of the same person is less than the variability between persons.[116] Ideally, the results of this comparison process should make a clear distinction between the results from the comparison of the same characteristics and those from the comparison of other characteristics (from the same or another data subject). However, in reality, most systems deliver results which have a more or less important *overlap region*. For this reason, a so called *threshold value* is used. The choice of this value, as further explained in § 119, determines the security and the convenience of a specific biometric system.

2.2.2.4.3 Decision

106. This third step uses the outcome of the comparison to declare a result. The decision will be taken in accordance with application dependent criteria, including the decision threshold (see *below*).

107. For biometric systems, and depending on the identification or verification functionality of a system, there are two kinds of decisions. There is a biometric *verification* decision, which is the 'comparison decision determining the validity of a biometric *claim* in a verification transaction' and a biometric *identification* decision which is a 'comparison decision as to whether a biometric reference(s) of a particular biometric data subject is in a biometric reference database' or not.[117]

---

[114] For example, if biometric data is already available (e.g., facial images from a surveillance video or from a watch list) and the query samples are compared with these data.

[115] See M. Bromba, *On the reconstruction of biometric raw data from template data*, 2006, available at http://www.bromba.com/knowhow/temppriv.htm

[116] See also, e.g., NRC, Biometric Recognition, 2010, pp. 28–30.

[117] See the terms 37.03.23 and 37.03.12 ISO Vocabulary for Biometrics 2012. About this important distinction between the verification and identification functionality, see also *above*, §§ 85–90 and footnotes 81–85.

On the application level, the system will make a decision as to whether the data subject is accepted or rejected. The complex way of decision making in biometric systems will be further explained *below*.

108. Upon successful comparison, additional data about the data subject may be released.[118]

2.2.2.5 Biometric System Errors

109. A biometric system captures the biological or behavioral characteristics of an individual through a measurement process with the aim of arriving at a realistic and invariant representation of the biometric characteristic for discerning the unique or distinctive information. This measurement process is *intrinsically error prone*.[119] Errors occur in fact at every step of the process. It starts from the very first phase. For example, a biometric characteristic will for comparison rarely (in fact almost never) be *presented* in the same way as it was acquired during enrolment and the interaction of the individual with the system will always be different.[120] Furthermore, in case of a bad quality sample, it will not be possible to *extract* relevant features for later comparison. In case the features prove to contain insufficient distinctive information, the template creation may fail. Last, but not least, there may be an error in the *comparison*.

110. The measurement process involves the use of *algorithms* for the biometric feature *extraction* and algorithms for the *comparison* of the real-time input[121] data from the data subject against the reference template(s) or image(s).[122] Because of the variability of the submission of biometric characteristics which need to be compared in a biometric system with pre-established characteristics which were registered upon enrolment, algorithms have a very important role in each of

[118] This information would be released typically from the identity database or the BIR.

[119] See also NRC, Biometric Recognition, 2010, p. 3: '[b]iometric recognition systems are inherently probabilistic, and their performance needs to be assessed within the context of this fundamental and critical characteristic.'

[120] For example, an individual will present his or her fingers always in a (slightly) different angle on a scanner, or present a fingertip instead of the central pad of the finger or use more pressure. The capture will be affected by numerous other factors (e.g., dust, sweat, …) or changes (e.g., by age, environment, disease, training of the person, intentional alterations, …). Because of this and other inconsistent conditions, for example a cold or sweaty hand, and varying circumstances (high humidity because of the season, …), the measurement of the characteristic may differ or produce errors. About the importance of these intra-class variations, see also NRC, Biometric Recognition, 2010, p. 5.

[121] Also referred to above as the submitted biometric data or the 'fresh' biometric data.

[122] An algorithm is a mathematical or logical procedure for solving a problem. An algorithm is in fact a 'recipe' for finding the right answer to a difficult problem by breaking down the problem into simple steps. See, e.g., B. Pfaffenberger, *Que's Computer and Internet Dictionary*, 1995, Que, p. 15. About algorithms, see also, e.g., B. Preneel, 'An Introduction to Modern Cryptology', June 2007, pp. 19–25 ('Preneel, Modern Cryptology, 2007').

the measurement and comparison processes. The algorithms and the systematic and statistical errors of the measurement define to an important extent the separation capability between different individuals and hence the benefits ànd limits of biometric system and applications.[123] The algorithms used are hence crucial in biometric systems and are in many cases proprietary, *i.e.* patented and owned or licensed by a company or held secret.

Some statistic errors are hereunder briefly explained. We hereunder limit ourselves to explaining some of the mostly used error concepts. While these concepts combined with abstract figures seem clear, there are several aspects to errors and accuracy rates, including difficulties relating to the testing of systems, which illustrate the complexity of biometric systems.

2.2.2.5.1 Statistical Measurements, Failures and Errors of Biometric Systems

111. Some of the failure concepts in relation to biometric systems are hereunder described in a very concise way. For a complete and detailed description of these failures and other error concepts, we refer to specialized books and articles by experts dedicated to the performance of particular biometric characteristics and systems and containing very detailed information about possible errors and the way to analyze and restrict them.[124]

2.2.2.5.2 Failure to Enroll

112. During the enrolment process, there is a *probability* that the system will *fail to create a reference* sample or template in some cases. This failure may be caused by the fact that the data subject misses a required characteristic, e.g., the missing of particular fingers because of an accident, or that the characteristic has been damaged.[125]

This is referred to as a failure to enroll (FTE). Fingerprint, for example, may have a high FTE, as compared to other methods. The FTE will in principle also be determined by the *enrolment policy*, which will define the maximum number of presentations and attempts that the data subject may make. The FTE rate would – according

[123] Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, p. 26.

[124] See, for example, Maltoni, Maio, Jain and Prabhakar, Handbook Fingerprint, 2009, pp. 11–22; for a succinct and more general overview, see, e.g., Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, pp. 26–36.

[125] For example, damage to hands and/or fingers of manual labor workers or of elder individuals and damage to (all) finger tips because of repeated use for glucose monitoring tests (for example by (an increasing number of) diabetes patients). The failure to create a reference template could also be due to the fact that not enough distinctive information can be processed or because the quality of the image is poor. This quality may also be influenced by the factors just mentioned or other conditions, including weather conditions, such as warm or cold weather.

to the definition in the ISO Vocabulary for Biometrics – in principle be based on the number of transactions,[126] not including the number of data subjects not being able to submit because the characteristic is not present.[127]

113. The data controller or any other controller of the system could decide to disable the FTE. In that case, templates of poor quality will be stored, producing more errors upon comparison.

2.2.2.5.3 Failure to Acquire

114. There is also a probability that a system *fails to acquire* (FTA) a given biometric characteristic *for subsequent comparison*. This is the case if the output of the automated data capture process can not be accepted.[128] This failure can occur during the capture or extract steps of the enrolment or the later comparison. The FTA rate is the relative frequency that either the capture or the extract process *could not complete its task in a sufficient quality*.[129] The failure includes the probability of the failures to capture (FTC) and of the failures to compare (FTM[130]).

2.2.2.5.4 Errors: FAR- FRR/FMR-FNMR

115. Once the characteristic is acquired, the biometric system risks during the statistical measurement comparison inherently to produce errors. A false acceptance error will occur when an acquired sample or template from one individual is erroneously decided as matching an enrolled sample or template from another individual. A false rejection error will occur when an acquired sample or template from one individual is erroneously decided as not matching with an enrolled sample or template from the same individual. It is clear that *false acceptance errors and false rejection errors*, depending on the claim made, *compromise the security* or *convenience* of a biometric system. They also affect the legitimate data subjects, who have to re-attempt and start the biometric comparison process again (in case of a positive claim) or are erroneously singled out as being a listed suspect (in case of a negative claim).

116. The rates associated with these errors are the false acceptance rates (FAR) and the false rejection rates (FRR) of a given system. The FAR and FRR are *interrelated*: decreasing the FAR of a biometric system will make that the FRR increases

---

[126] During a comparison step, one or several transactions using a particular characteristic may be effectuated or needed to complete the comparison.

[127] See term 37.09.05 ISO Vocabulary for Biometrics 2012. Because it would not include the number of data subjects which are unable to provide the characteristics, the rate based on the number of transactions will be more advantageous.

[128] For example, the fingerprint area is too small.

[129] Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, p. 21.

[130] See *below* § 117.

and *vice versa*. They will in fact relate to and therefore be determined by the system threshold which may be chosen by the data controller and that the system hence needs to meet. For high security applications deploying positive claims, the FAR shall be set to a minimum (because having unauthorized persons accepted is highly undesirable), but this will imply that the FRR will increase (implying that authorized persons are falsely rejected). In practice, systems have non-zero FAR and FRR.[131]

False acceptance rates (FAR) and false rejection rates (FRR) will overall be used to indicate the performance of a system or a practical implementation. Their use is popular, especially in the commercial sector. They refer to the *performance of the full comparison* process including *all steps* (e.g., including whether various capture attempts are accepted by the decision policy) until the final decision by the system. They are in principle *decision errors*. They shall also be seen in relation to the functionality of the comparison process (verification or identification) and the application.[132] The rates further depend on the biometric *characteristic used* by the system. Hand geometry, for example, has a high FAR using the identification functionality, as compared to other biometric characteristics. A very important aspect as well is the *quality* of the data stored and used for the comparison. Other specifications of the system will determine the rates as well. We will expand on what we could call the volatility of the error rates and its intransparency in Part II and III, as one of the risks of the use of biometric systems.

In general, the FRR for most biometric systems will range from being falsely rejected (on average) one out of five times up to one for every thousand times, i.e., FRR being 20 % down to 0.1 %. The FAR seems to range on average from one out of hundred times for low security applications, up to about one for every ten million, the latter for (very) high security applications, i.e. a FAR respectively at 1 % and at 0.00001 %.[133] Although a system with a FRR at 0.01 % and

[131] See A. Jain, *Improve biometrics adaptation for cryptographic techniques*, 17.01.2011, slide 5, presentation at the Turbine public workshop, available at http://www.turbine-project.eu/workshop_presentations.php

[132] As stated, the kind of decision (and the errors therein) will depend on the kind of claim made. It means that false acceptances and false rejections will result in different decisions depending on the claim made. In the case of a positive claim of identity, a false comparison decision will result in a false acceptance of the impostor, while in case of a negative claim, e.g., a comparison against a watch-list, a false comparison decision will result in a false rejection of a genuine claim. In case a database is used for comparison for a claim of non-identity (e.g., that a person is not on the watch list) or for a claim of identity (e.g., that person is enrolled as holder of a passport), the FAR will refer to the *expected proportion of decisions* that are incorrectly confirmed. The FAR is hence resulting in different decisions depending on the claim made and hence the application. FNMR and FMR (see *below*) to the contrary, are not application dependent.

[133] These figures were mentioned in 2007 in A. Cavoukian and A. Stoianov, *Biometric encryption : a positive-sum technology that achieves strong authentication, security and privacy*, Information and Privacy Commissioner Ontario, 2007, p. 8, available at www.ipc.on.ca ('Cavoukian and Stoianov, Biometric encryption, 2007'). A high security application is for example a border control in an airport.

a FAR at 0.0001 %[134] may seem reasonable, this may be unacceptable or very hard to manage if the database consists of for example 50 million records, which would give 50 incorrectly confirmed claims of identity (or of non-identity, in case of a watch list) and 5,000 false rejects.[135]

117. The system error rates FAR and FRR may further deviate significantly from the more technical algorithm error rates, in particular the false matching rate (FMR) and the false non matching rate (FNMR). The FAR and the FRR are dependent on the system and decision protocols used (number of attempts to acquire, number of reference templates used for the comparison, etc.), while the FMR and FNMR are usually error rates *at the comparison algorithm level*. It is hence important to distinguish FAR and FRR from the technical notion of false match rate (FMR) and the false non-match rate (FNMR).[136] FNMR and FMR are not application dependent and are in fact used and are *of technical importance* for the benchmarking of a specific biometric method.[137]

2.2.2.5.5 Biometric Systems and 'Decision Making Landscape'

118. As stated, depending on the type of application, for example a commercial biometric application such as a payment system, one may be willing to limit the possibilities of FRR as they may create customer nuisance, while accepting the costs of FAR. In other applications, for example in high security applications or applications in the public sector (e.g., for a national ID system), a high FAR may not be tolerated and is to be limited as much as desirable. *Decisions will hence have to be taken* when deploying biometric systems in an operational environment. The notion of 'decision landscape' has been used in order to portray the degree to which any improvement in one error rate must be paid for by a worsening in the other.[138] The criteria which will

---

[134] These rates mean that the system will compare on average the query data 9,999 times out of 10,000 times with the correct enrolled data and accept only once out of one million times falsely. For other FMR suggested by experts, see *below* Table 2.1.

[135] For a same reasoning, see Cavoukian and Stoianov, Biometric encryption 2007, p. 8. An example of where this type of large scale biometric system would be used is at airports with the passage of millions of travelers every day. The error rates mentioned, however, are rather low and it could be hard to achieve these rates with a single characteristic only.

[136] FMR could generally be explained as the likelihood that biometric measurements of two different persons falsely match, while FNMR as the likelihood that the biometric measurements from one and the same person fail to match at later occasions.

[137] L. Müller and E. Kindt (eds.), *D3.14 Model implementation for a user controlled biometric authentication*, Frankfurt, FIDIS, August 2009, p. 10 ('Müller and Kindt, Model implementation, Fidis, D.3.14, 2009'). This distinction is not always made. See, e.g., Irish Council for Bioethics, *Biometrics : Enhancing security or invading privacy ? Opinion*, 2009, p. 8, footnote 86 which equals FAR with the FMR and the FRR with the FNMR ('Irish Council, Biometrics, 2009').

[138] J. Daugman, *Biometric decision landscapes. Technical Report 482*, Cambridge, University of Cambridge Computer Laboratory, January 2000, p. 1, available at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-482.pdf

play a role are hereunder reiterated. Another aspect is that information about the frequency of false claims (impostors) is also important in order to know the probability that any given recognition by the system is in error.[139]

2.2.2.5.6 Threshold

119. The decision threshold ('*drempel*'/'*seuil d'acceptation*') is the minimum value that a biometric comparison process shall reach. It is chosen in order to optimize error rates[140] of a system in function of application requirements.

The acceptance or rejection decision of the system upon the comparison is calculated by comparing the answer of the system to the threshold. Tightening the decision threshold would generally mean increasing the FRR and decreasing the FAR. Slackening the threshold would decrease the FRR and increase the FAR.[141] This threshold is configured by the administrator[142] of the system, by the developer or vendor of the system.[143] Data subjects have usually no impact and no idea of the error rates and of the threshold set in case they are not explicitly informed thereof.

120. For illustration purposes, experts have suggested that *depending on the use case and on the security requirements of a system*, accuracy performance, in particular FMR, in public large scale applications, which shall be taken into account in the setting of the thresholds, could be presented as follows (Table 2.1):

2.2.2.5.7 Equal Error Rate ('EER') and the Receiver Operating Characteristic ('ROC') Curve

121. Because the manufacturer of a biometric system does not know for which application the system will be used, the performance of the system could be reflected by indicating where the FMR is equal to the FNMR, i.e. that the number or the proportion of the false matches is (approximately) equal to the number or the proportion of the false non matches. In such case, this error rate is referred to as the Equal

---

[139] On this issue, see NRC, Biometric Recognition, 2010, pp. 36–45. It is demonstrated that 'natural belief' and intuition in biometric systems is often wrong as the 'yes' decisions of a system also depend upon the impostor base rate (i.e. the probability that a randomly chosen individual presenting to the system will be an impostor).

[140] According to the definition in the ISO standard 19795-1, the global error rate may also include the failure to enroll rate (FTE) and the failure to acquire (FTA).

[141] See also *above*.

[142] This could be the controller of the data processing, the processor or any party or person appointed by either the controller or the processor. 'Controller' and 'processor' refer to the terms of the Directive 95/46/EC. For the definition, see respectively Art. 2(d) and Art. 2(e) Directive 95/46/EC.

[143] Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, p. 24.

Table 2.1 False acceptance requirements suggested for particular systems by the National Physical Laboratory (U.K.)[a]

Type of application	FMR should be lower than :
National ID card system for eliminating double identities	1 in 10^{10}–10^{12}
National watch list	1 in 10^{7}–10^{9}
Verification functionality in an open system	1 in 10^{4}–10^{6}
Verification functionality in a closed system	1 in 1,000

[a]T. Mansfield, *Public Domain Biometric Applications. Functionality – Performance – Scalability*, presentation, slide 11, NPL, 2004, available at http://www.cesg.gov.uk/policyguidance/biometrics/Pages/Government-Biometrics-Workshop.aspx. The figures '1 in 10^{4}–10^{6}', e.g., mean that the false matches should be lower than one out of ten thousand (10,000) up to one out of one million (1,000,000). The threshold figures for a national ID card system refer to the population of a large national country. For an open system, reference is made to the example of services obtained with a biometric ID card. For a closed system, reference is made to access control to a building

Error Rate or EER. The EER (i.e. the error rate when FMR ≈ FNMR) is a *measure* used *for the quality* of a biometric system that operates in a common commercial or civilian environment.[144]

122. Diagrams or curves are used in order to obtain a graphical view of the error rates. An example is the Receiver Operating Characteristic ('ROC') curve which shows the FNMR (FRR) in function of the FMR (FAR). A typical ROC curve in relation with biometric applications, including the EER, is shown *below* in Fig. 2.6.

Diagrams are also used for testing and reporting purposes about the error rates of multiple tested biometric algorithms or systems. According to the ISO 19795-1 testing standard, the Detection Error Trade-Off ('DET') curve which is a ROC type curve[145] shall show the FNMR (FRR) in function of the FMR (FAR), including the EER.

2.2.2.5.8 Tunable Trust

123. In order to increase the performance of a system with a given FAR, it has been researched and tested to what extent the use of more information from biometric characteristics (e.g., two fingerprints instead of one[146]) can improve the FRR. In this case, although more biometric characteristics are requested, the trust in the

[144]For high security or forensic applications, the EER is not a good quality indicator. For such applications, the FMR or the FNMR are the dominant criteria.

[145]ROC and DET curves typically compare two operating characteristics as criteria change. ROC and DET curves, developed and used first by electrical engineers, are used now in various domains, including medicine, and also for biometric systems.

[146]Two fingerprints have more discriminating features (minutiae, ..) and permit to set a tighter threshold with improved error rates.

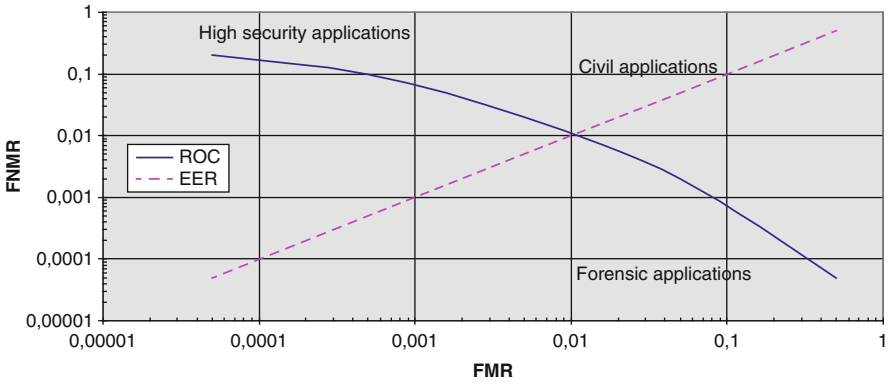

Fig. 2.6 Typical ROC curve (Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, p. 33; see also E. Kindt, L. Müller and M. Meints, '4.2.3. Biometrics', in K. Rannenberg, D. Royer and A. Deuker (eds.), *The Future of Identity in the Information Society-Challenges and Opportunities*, Dordrecht, Springer, 2009, (138), pp. 140–141 ('Kindt, Müller and Meints, 4.2.3. Biometrics, 2009'))

biometric system may increase because of better error rates and effectiveness of the system.[147] Tunable trust allows on the other hand to limit the collection of biometric data, for example for low security zones.

2.2.2.5.9 General System Performances for Specific Biometric Characteristics

124. The controller will have to choose the most apt biometric system for the application envisaged. Important and decisive factors for the controller will usually be *cost* and *reliability* of the system. Other considerations may be privacy aspects of the biometric characteristic used and acceptance by the public. The *performance* of the system, however, will play an important role as well. Performance and accuracy is moreover also of the *essence* in the discussion of the *need* for and the *effectiveness* of a biometric system in relation with the purposes envisaged.[148]

125. The evaluation of the performance of a particular system, however, is a complex issue. First, the general performances of the various systems using a particular biometric characteristics will differ because of a multitude of factors and of

[147] This concept of 'tunable trust' was for example researched in the EU-funded project TrUsted Revocable Biometric IdeNtitiEs project (TURBINE) (2008–2011) (7th Framework programme), at www.turbine-project.eu ('Turbine').

[148] Because biometric systems may interfere with fundamental rights, such as privacy and data protection, infringements will have to be necessary and proportionate. For this purpose, the controller will have to demonstrate that the system is, in addition to being necessary, relevant ànd sufficient. This is further analyzed and discussed in Part II.

'variables' that can be set or chosen, including the environment where the system is used, the variability of the biometric characteristic used, the biometric capture and comparison process, the components of the system, the functionality chosen (identification as compared to verification), and the size of the database (especially for identification), the (limited) storage and processing capacities, and the performance of (proprietary) algorithms.[149] In fact, there is even an *inability to predict performance in one environment from measurements of performance in another environment*.[150]

In addition, it remains very difficult to have an accurate view of the performance results of biometric systems because of different approaches for the testing of a biometric system, as we will explain later.

126. We nevertheless attempt to summarize hereunder in general the current state of the art in terms of performance for specific biometric characteristics.[151] A detailed discussion nor overview is within the scope of this book.[152] However, having a grasp of the accuracy of the measurements in function of the threshold set for particular biometric characteristics is useful for our discussion. This is often overlooked in debates and decisions to implement biometric systems,[153] while this is relevant in order to evaluate the security offered by a system and accuracy needs to be balanced with the privacy rights of the data subjects involved. It is further of great importance for the controller deciding for a particular system for a given situation.

---

[149] For an overview of factors which influence performance, such as relating to population demographics, user physiology and user appearance, but also relating to the technical components of a biometric system, see A. Mansfield and J. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, August 2002, pp. 28–30 (Annex A), ('Mansfield and Wayman, Best Practices in Testing and Reporting, 2002'), available at http://www.sas.el.utwente.nl/open/courses/intro_biometrics/Mansfield02.pdf

[150] J. Wayman, *Biometrics & how they work*, San Jose State University, 2002, available at http://www.cfp2002.org/proceedings/proceedings/jlwcfp2002.pdf; about performance evaluation before and around 2005 for the four most used characteristics (iris, facial image, fingerprint and voice), see also Wayman, Jain, Maltoni, Maio, Biometric systems, 2005, pp. 21–262.

[151] Because there is a constant refinement in biometric technology, such as in terms of the capture devices and the comparison algorithms used, these performance results are continuously changing and improving. The overview may therefore not be fully up to data. Specialized works should be consulted for this purpose.

[152] For up to date information on performance of biometric systems, testing results of specialized and by preference independent research centers shall be consulted. See in this regard e.g., the Biometric System Laboratory at the University of Bologna, devoted mainly to fingerprint and face recognition, with website at http://biolab.csr.unibo.it/home.asp; see also the information provided by the Research lab and group on Biometrics of the Department of Computer Science and Engineering of the Michigan State University, available at http://www.cse.msu.edu/rgroups/biometrics/

[153] E.g., the decision by the EU Council of Ministers for the mandatory inclusion of facial images in ePassports in 2004 (see also Part III), while face recognition technology was not satisfactory. See also the homepage of the 3Dface project, available at http://www.3dface.org/home/welcome.html

2.2.2.5.10 Examples of the Performance for Various Biometric Characteristics

127. The performance of biometric systems using various characteristics has been reported on in the last decade by a multitude of interested stakeholders, such as vendors and (vendor) associations, but also by national (governmental) institutions, other interested parties and research institutions. It is – as far as we know – therefore not possible to give a single overview of biometric performance for a particular characteristic. Moreover, such overviews risk to become soon obsolete. We will therefore to the extent possible give hereunder only *some general idea* on the performance of some selected biometric characteristics as researched and mention *some factors* which may influence such performance.[154]

Moreover, it should be noted that the *performance evaluation can be done at various levels*. The experts make a distinction between '*technology evaluation*', which consists primarily of the evaluation of competing algorithms on a standardized database with characteristics collected with a general sensor, '*scenario evaluation*' which is to determine the overall system performance in a prototype or simulated application, and '*operational evaluation*', which is the testing of a complete biometric system in a specific environment with a specific target population.[155] The latter type of evaluation, which we would name generally system performance, would in principle be of interest for a controller and the data subjects. Only the first type of evaluation, however, allows to repeat the testing results.

128. The use of *fingerprint* in a civil biometric comparison system usually provides good results. These results are also improving. In 2004, 'state-of-the-art' error rates for fingerprint verification were reported between 0.1 and 2 % FRR and 1 up to 2 % FAR.[156] Using an increasing number of fingers (up to ten) will improve the results of such system in a manner that is correlated to the number of fingers measured.

The performance of *facial recognition systems* is considerably influenced by pose variation, illumination conditions (during day or night, indoor or outdoor), distance and camera position, but also by aging as well as the cooperation of the data subject. Therefore, the performance, especially in a 1: n system, was initially rather poor but is improving. For example, in 2010, a success rate of 91 % was mentioned as a best case result in a proof of concept testing of a face recognition project with identification functionality and privacy protective technology involving up to

---

[154] It remains, however, very difficult to represent generally the performance for a particular characteristic, because the use of additional information, as well as further developments of the technology, may impact the rates. See, e.g., about the use of spectral minutiae representations for fingerprint, a rather novel method to represent a minutiae set as a fixed-length feature vector or a binary string, in combination with template protection (see Part III), and the rates obtained in Xu, Spectral Minutiae Representations, 2010.

[155] Mansfield and Wayman, Best Practices in Testing and Reporting, 2002, pp. 3–4.

[156] See A. Jain, *Biometric System Security*, Michigan, Dept. of Computer Science and Engineering. Michigan State University, at slide 12 of the presentation previously available at http://www.cse.msu.edu referring to the Fingerprint Vendor Technology Evaluation (FpVTE) of 2003 of NIST and the Fingerprint Verification Competition (FVC) of 2004 (about the FVCs, see also footnote 177 *below*).

20,000 visitors per day.[157] This is an improvement as compared to the results of a the test in a railway station in an operational environment by the German Federal Criminal Police Office in 2007 reporting a success rate of using identification against a watch list of 30–60 % as tested.[158]

At the Face Recognition Vendor Test (FRVT) competition organized by the National Institute of Standards and Technology (NIST) (U.S.A.),[159] improvements for some algorithms for face recognition were at a fixed FMR of 0.001 in 2006 reported to be 0.026 FNMR and in 2010 up to 0.003 FNMR.[160] These rates, however, are not comparable with other rates for face recognition, for example applied on passport photos, where the accuracy is still rather low.[161]

For *iris*, the technology provides good accuracy rates because of the great deal of random variation amongst different persons in the detailed iris patterns. Because iris patterns have so *much complexity*[162] *and randomness*, iris technology is very *robust*

---

[157] See A. Cavoukian and T. Marinelli, *Privacy-Protective Facial Recognition*: *Biometric Encryption*. *Proof of Concept*, Information and Privacy Commissioner Ontario, Ontario Lottery and Gaming Corporation, November 2010, p. 13 ('Cavoukian and Marinelli, Privacy-Protective Facial Recognition, 2010'), available at www.ipc.on.ca. In this paper, the Information and Privacy Commissioner of Ontario, Canada ('IPC, Ontario') describes a proof of concept for privacy-protective facial recognition, applying biometric encryption (see Part III). The IPC, Ontario therein mentions for face recognition technology applied in a casino environment for a self-exclusion program, an increase in the project (due to correction of lighting, camera position but also "attention-getting" devices like marketing screens) from approximately 30 % to 91 % Correct Identification Rate (CIR) (this new term is probably used because, in contrast with many biometric systems, the scenario required a minimized FRR (self-excluded individuals want to be recognized), while maintaining an acceptable FAR).

[158] See Bundeskriminalamt, *Forschungsprojekt*. *Gesichtserkennung als Fahndungshilfsmittel Foto-Fahndung*. *Abschlussbericht*, Wiesbaden, February 2007, 28 p. ('Bundeskriminalamt, Forschungsprojekt. Gesichtserkennung, 2007').

[159] About NIST and this and similar 'performance competitions', see also *below* and at footnote 160 and Part III Chap. 7, § 171.

[160] P. Grother, G. Quinn and P. Phillips, *Multiple-Biometric Evaluation* (*MBE*) – *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709, 2010, p. 34 ('Grother, Quinn and Phillips, Multiple Biometric Evaluation (MBE), 2010'), available at http://biometrics.nist.gov/cs_links/face/mbe/MBE_2D_face_report_NISTIR_7709.pdf. Compare with previous results of face recognition in 2002 at the Face Recognition Vendor Test (FRVT) 2002 competition, mentioning for the best-performing systems an error rate of 10 % at a FAR of 1 % for verification under indoor conditions. At a FAR of 0.1 %, the two top systems had error rates of 18 % (see JRC, Biometrics at the Frontiers, 2005, p. 107). Compare in addition with the error rates set for 3D facial recognition in the 3D Face project, in particular a FAR of less than 0.25 % and a FRR of less than 2.5 % and the results of the researched facial comparison techniques and pilots, as reported in C. Bush, *Forschung für die Grenzkontrollen der Zukunft*, 2009, Darmstadt, Hochschule Darmstadt, 2009, p. 10, available at https://www.fbi.h-da.de/fileadmin/gruppen/FG-IT-Sicherheit/Publikationen/2009/h_da_querschnitt-090403.pdf

[161] See T. Bourlai, A. Ross and A. Jain, 'On Matching Digital Face Images Against Scanned Passport Photos', in *Proc*. *of First IEEE Intern*. *Conf*. *on Biometrics*, *Identity and Security*, September 2009, p. 9, also available at http://www.cse.msu.edu/rgroups/biometrics/Publications/Face/BourlaiRossJain_BIDS2009.pdf ('Bourlai, Ross and Jain, Matching Digital Face Images, 2009').

[162] Its complexity allows that iris technology generally compares multiple times more points as compared to, e.g., the fingerprint technology.

against making false acceptances. This robustness against false acceptances allows that the technology can replace identity controls without any document or card to be handed over and that iris patterns are used in large-scale applications which deploy identification.[163] Early 2011, the best performances for iris at a fixed FMR of 0.001 have an average of 0.0146 FNMR out of 10,000.[164] On the other hand, the iris patterns are so complex that comparison needs to be left to a biometric system as they can not be verified manually.

For *hand geometry*, results may be influenced by for example (young) age, position of the data subject (standing or sitting) and the wearing of jewellery. Because hand geometry is not unique, it is mainly used deploying the verification functionality providing acceptable results while application in large-scale identity applications is limited.[165]

Voice results are affected by changing behavior but are improving as well. In 2004, 'state-of-the-art' error rates for voice were reported to be between 5 up to 10 % FRR and 2 up to 5 % FAR. Partly because of advanced algorithms, *inter alia* to deal with speaker variants and enabling fusion of the output of multiple algorithms, and improved hardware, missed detection error rate (see *above*) has dropped from 16 % in 2006 to about 7 % in 2010.[166]

129. Typical performance for large scale biometric applications has been researched by various institutions in countries where such large scale applications were planned or were introduced.[167] It was found that particular biometric characteristics could give typically the following results (Table 2.2):

---

[163] Iris recognition is – comparable to other biometric characteristics – mainly used in two ways: the determination of a person's identity by searching a database of enrolled iris patterns or screening against a watch list of undesired identities registered. In the United Arab Emirates, for example, it is used for screening foreign nationals who require a visa against the watch-list. In 2008, about 60 million persons were enrolled in iris recognition systems in the world. See J. Daugman, 'Interview. Pattern recognition : Biometrics, Identity and the State – An Interview with John Daugman', in *BioScieties* 2008, pp. 81–82. J. Daugman is the inventor of the 'IrisCode', the iris recognition algorithm, that was patented.

[164] See E. Newton, *Large-scale Evaluation of Biometric Algorithms*, slide 11, presentation at CryptoBiometrics for Enhanced Trusted Identity Management: Dreams and Reality, 17–18.01.2011, Turbine final public workshop, Brussels, Turbine, available at http://www.turbine-project.eu/workshop_presentations.php ('Newton, Large-scale evaluation, 2011').

[165] See, Jain, Ross, Pankanti, Hand Geometry, 1999.

[166] NSTC, National Biometrics Challenge, 2011, p. 14 with references to the NIST Speaker Recognition Evaluation; see also A. Jain, *Biometric System Security*, Michigan, Dept. of Computer Science and Engineering. Michigan State University, previously at slide 12 of the presentation previously available at http://www.cse.msu.edu

[167] For example, in the United States, which introduced the US-VISIT program (see below), biometric technology is researched and the performance tested by the National Institute for Standards and Technology (NIST). In the United Kingdom, which planned to introduce an ID card scheme, research was conducted by the National Physical Laboratory (NPL). About research of the NPL for the fore mentioned ID card scheme, see, e.g., London School of Economics and Political Science, *The Identity Project. An assessment of the UK Identity Cards Bill and its implications*, London, LSE. The Department of Information Systems, v. 1.09, 27 June, 2005, pp. 172–174 ('LSE, Identity Project, 2005'), available at http://is2.lse.ac.uk/IDcard/identityreport.pdf

Table 2.2 Overview of typical performances presented by the National Physical Laboratory (U.K.) for some biometric characteristics in applications in the public sector[a]

Biometric characteristic	FTE	FMR	FNM
Face	0	1 %	2 %
Iris	0.5 %	1 in 10^6	1 %
Fingerprint (one)	1 %	1 in 10^5	2 %
Fingerprint (ten)	Less than 0.1 %	1 in 10^{11}	1 %

[a]T. Mansfield, *Public Domain Biometric Applications. Functionality – Performance – Scalability*, presentation, slide 6, NPL, 2004, available at http://www.cesg.gov.uk/policyguidance/biometrics/Pages/Government-Biometrics-Workshop.aspx. The exact year of the testing, which remains relevant, is not known (but may be around 2004), as well as the population for which the results would be valid (although this could be the U.K. population or about 60 million). For iris performance, see also Matey et al., Iris on the Move, 2006, p. 1937

2.2.2.5.11 Typical Problems and Issues for Large Scale Biometric Implementations

130. Large scale biometric systems usually deploy the *identification* mode which identifies the data subjects and which in addition offers the advantages of allowing a duplicate enrolment check (e.g., systems for issuing an identity document or for obtaining a social benefit) or a comparison against a watch list (see *above* § 86). Large scale biometric systems however encounter some typical problems. First of all, it is necessary to understand that, because of the comparison with the many stored references and the possible *overlap* of the representation of the distinctive extracted features (e.g., of a large population), the use of the identification functionality demands much more from the measurement and comparison algorithms in order to give good results notwithstanding the interclass variability.[168] *Error rates* for large scale systems will also have a greater impact because of the high number of people subjected to the system (see *above* § 89 and § 116). The systems are furthermore often designed and developed without a thorough testing of the technology using a similar large number of enrolled data subjects. The *scaling* to a larger set of the test results typically on a smaller set of data has proven to be problematic and the error rates therefore difficult to predict.[169] Furthermore, the databases of

[168] See also *above* §§ 89 and 105; it is possible nor the aim to explain in detail the various consequences of the use of a large scale biometric system in identification mode on errors. We refer in this respect to the many publications by experts on the matter, some of which are cited herein (see, e.g., footnotes 116, 169 and 170). For a succinct discussion of the matter, see also, e.g., L. Müller, Reference model of a biometric system, in Kindt and Müller, Biometrics in identity management, Fidis, D.3.10, 2007, pp. 26–27.

[169] See also about this gap in testing biometric systems for larger scale applications, whereby largest tests performed are on databases with less than 200,000 data subjects, and most in verification mode, Newton, Large-scale evaluation, 2011, slide 8. For further reading about this problem, see, e.g., H. Jarosz and J.-Ch. Fondeur, 'Large-Scale Identification System Design', in J. Wayman, A. Jain, D. Maltoni, D. Maio (eds.), Biometric systems: Technology, Design, and Performance Evaluation, New York, Springer, 2005, (263), pp. 266–279.

large scale systems risk to contain data which are obsolete, incorrect or which do not meet minimum *quality* requirements (if any).[170]

2.2.2.5.12 Need for Independent Testing and Evaluation

131. Indications about the performance of a biometric system are usually provided by the vendor of a system in terms of FAR and FRR. These errors rates will be based upon specific presumptions made by the vendor, such as the operating conditions, including but not limited to the number of data subjects to enroll,[171] and the quality of the data captured. However, we itinerate that *various factors influence the performance* of a system. Many of these factors relate directly to the system and the application, including for example the functionality used (verification or identification), the scale (and scalability[172]) and protective measures,[173] but also to elements such as the distinctiveness of the characteristic used. Other factors relate to the context in which a system is used, e.g., the 'noise' due to poor lightning conditions, or inexperienced (or non cooperative) data subjects, resulting in for example a higher number of incorrectly placed fingers, and therefore lower performance.[174] Another factor is the temporal change of particular characteristics, for example because of illness or age. Performance for fingerprint of aged persons may be much worse than for a population with younger subjects.

132. Because of the multitude of factors that influences the results and performance of a biometric system, *independent testing and evaluation* of a system is needed in order to provide information about the performance and hence indirectly about the fitness for a finality, such as the security, that a system aims to provide. The testing should include the measuring of the accuracy of the algorithms, not only in relation

---

[170] About large-scale biometric systems in Europe, and the issues involved, see also, e.g., P. Rotter (ed.), *Large-scale Biometrics Deployment in Europe*: *Identifying Challenges and Threats*, JRC Scientific and Technical Reports, European Commission JRC – IPTS, Seville, 2008, 135 p. ('JRC, Report Large-scale Biometrics Deployment, 2008'); see also about the ePassport in the Netherlands, discussed in Part III.

[171] However, it is almost not possible to make any assumptions about the number of impostors, which will also play a role.

[172] With scalability, briefly mentioned in § 130, we refer to the possibility to use a particular biometric solution for a higher number of individuals. A particular biometric solution is often tested with a small number of persons. It is generally recognized that, especially for the identification functionality, the test results obtained on a smaller set of data cannot be easily scaled to predict results for a wider population. Testing for obtaining reliable results for a higher number of persons involved is difficult, because of the limited availability of large biometric databases for testing purposes.

[173] For example, the use of so-called cryptobiometric technologies. See Part III.

[174] For a discussion of testing and issues of performance for various characteristics (with results valid in 2003), see also, e.g., M. Rejman-Greene (ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 October 2003, pp. 90–122 ('Rejman-Green, BioVision Roadmap, 2003'), available at http://oai.cwi.nl/oai/asset/4057/04057D.pdf

to the biometric data of the vendor, but also *in relation with an independent data set*.[175] Furthermore, the testing should include the context specific conditions as well as vulnerabilities.

It is also of crucial important to understand and to retain that the testing and evaluation of biometric systems can be done on three levels: (1) on the level of the algorithms for the comparison, (2) on the level of a scenario implemented in a particular prototype or pilot test and (3) on the level of a system in an operational environment. Evaluations done on the algorithm level will – although they may give an indication – rarely provide a correct report of the error results of *biometric systems in an operational environment*. Moreover, while test result on the first level should generally be repeatable, this is not the case for performance results in an operational environment. Results of testing and of the error rates should hence be given and interpreted in the correct context.

133. The testing of the performance of a biometric system should also follow a sound *methodology*. Evaluation has to some degree already been subject to some standardization[176] but the methodology to follow remains in general extensively discussed and debated.

134. In order to allow the setting of benchmarks, biometric databases are made publicly available for testing purposes during so-called competitions. For example, for fingerprint, 'Fingerprint Verification Competitions' ('FVCs') are organized, allowing suppliers of biometric systems to compare the results of their algorithms on the same set of fingerprint data.[177] Similar initiatives for other characteristics are taken as well, for example for face recognition, of which the reports are equally published, and projects are set up for the development and the making available of

[175] This dataset could be a publicly available dataset or a dataset which is not accessible to third parties (and hence 'sequestered' because it is only used by the performance evaluators). See also the objectives of the BEAT project, mentioned in footnote 178 *below*.

[176] ISO/IEC 19795-2:2007, for example, is a standard for testing methodologies for the evaluation of technology and scenario's. For a proposed method for vulnerability testing, see, e.g., the Vulnerability Assessment Expert Group of the Australian Biometrics Institute and its work.

[177] See, e.g., the FVC 2000 (the first International Fingerprint Verification Competition), and the FVC 2002, FVC 2004 and FVC 2006 competitions. For FVC 2002, see e.g., http://bias.csr.unibo.it/fvc2002. A database with fingerprints is made publicly available for 'training' of the algorithms (such database is for example made available on a DVD included in a publicly available handbook on fingerprint recognition). The evaluation is thereafter made by the organizers on a sequestered database. The completion allows to set a common benchmark for algorithms, allowing to compare. Online evaluation is the latest evolution of the FVC. See FVC-onGoing, a webbased automated evaluation for fingerprint recognition algorithms, available at https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx. For other publicly available databases, see, e.g., the U.S. National Institute for Standards and Technology (NIST) Special Databases, e.g., NIST Special Database 4, commercially available at http://www.nist.gov/srd/nistsd4.cfm and the Fingerprint Vendor Technology Evaluation 2012 (FpVTE 2012) organized by NIST for evaluation of large one-to-many fingerprint identification algorithms (see http://www.nist.gov/itl/iad/ig/fpvte2012.cfm).

an open source online platform for transparent standard testing and evaluation of biometric algorithms for any interested parties.[178]

2.2.2.5.13 Acceptable False Accept and False Reject Rate?

135. Because of the high variety of the components and elements used in a biometric system (characteristics, sensors, extraction and comparison algorithms, fusion systems used, …) and ongoing discussions about the methodology for testing, an agreement on acceptable error rates let alone objective criteria remain difficult. Experts in the field however seem to generally agree that for a biometric *verification* comparison system with both strong security and convenience requirements, neither the false accept rate nor the false reject rate should exceed 0.1 %.[179] However, much will depend on the application.

136. In September 2008, the same renowned experts reported that, based upon evaluations made by the National Institute of Standards and Technology (NIST) in the period from 2003 to 2006, none of the biometric systems tested based on fingerprint, face, iris and voice reached the generally agreed aim of a false accept rate and false reject rate of being lower than 0.1 %.[180]

2.2.2.6 Multimodal Biometric Systems

137. In some cases, more than one biometric characteristic of the same data subject are combined and the results 'fused' *to improve performance*. Where the source of errors is for example the use of less distinctive characteristic, or in case of high performance requirements, (for example, for an identification application), the combination of two characteristics, e.g., two fingers, or the use of more than one type of characteristics, e.g., face and voice, generally improves the performance of the system. In case of risks of variability of data acquired during enrolment and data acquired for later comparison, which is the case especially for for example behavioral biometric characteristics (e.g., signature), multimodality improves the results. This use of multiple biometric characteristics is referred to as a multimodal

[178] See the objectives of the EU-funded Biometrics Evaluation and Testing (BEAT) project (2012–2016) (7th Framework programme), aimed at developing an open source online platform for use by multiple actors for the testing of algorithms in a transparent and independent way, with homepage available at http://www.beat-eu.org/. For benchmark initiatives for other characteristics, such as face recognition evaluations, see e.g., Rejman-Green, BioVision Roadmap, 2003, pp. 90–122.

[179] A. Jain and S. Pankanti, 'Beyond Fingerprinting. Security systems based on anatomical and behavioral characteristics may offer the best defense against identity theft', in *Scientific American* 2008, p. 80. ('Jain and Pankantin, Beyond Fingerprinting, 2008'). Ideal systems, however, do not exist. A system with a FAR and FRR of lower than 0.1 % may further rather point towards a system envisaged to offer security and not a membership validation system.

[180] Jain and Pankantin, Beyond Fingerprinting 2008, p. 81.

biometric systems system.[181] Another advantage of multimodality is that it may also reduce the errors caused by the 'noise' in systems or at least deter in some cases impostors and thieves[182] of biometric characteristics (which need in this case to do more efforts to 'steal' (e.g. by physical removing or by copying) more than one characteristic).

138. Multimodality, however, may also be of benefit in case a data subject is not able to submit one characteristic, for example because of illness or for religious reasons. Multimodal system which use more than one characteristic in parallel allowing more flexible use are therefore believed to have a potential to be more *socially inclusive*.[183]

2.2.3 Medical Aspects of Biometrics

139. Medical aspects of biometrics refer to possible so-called 'direct medical implications' in the form of (potential risks for) *damages* to one's health related to the use of biometric components of systems, especially scanning devices. For example, the use of biometric characteristics which require *physical contact* with the readers, such as fingerprints and hands, may contain a risk for potential germ transmission and contamination. This should be taken into account if the choice for a biometric system is to be made in a specific environment, for example, a hospital.

For retinal scanning and iris recognition, the concerns include that due to prolonged exposure to *infrared* (*or near-infrared*) *radiation* the eye may suffer thermal damage. Until now, reports state that it is believed though, until evidence of medical risks to the contrary, that the radiation absorbed is very low and that there are no significant implications for the eye.[184]

---

[181] The design of the multimodal system requires the so-called 'fusion' of the processing of the various characteristics. This can be done at various levels, e.g., at the level of the sensors, the scores, … See also JRC, Biometrics at the Frontiers, 2005, pp. 56–57. Various Union funded research projects explored the possibilities of multimodality. An example of such project is BioSec (see footnote 69). Another project was BioSecure (2004–20007) (see now the Association BioSecure, at http://biosecure.it-sudparis.eu/AB/). A system which uses multiple sources of biometric information, e.g., by multiple sensors to capture one biometric characteristic, multiple samples of the same, or allowing multiple instances, would be referred to as a multibiometric system. See on such systems, e.g., Li, S. (ed.), *Encyclopedia of Biometrics*, Springer, 2009, pp. 967–980 ('Li, Encyclopedia of Biometrics, 2009'). This distinction was not very clear in the WP 29 Opinion on developments in biometric technologies 2012 (WP193), p. 6, mentioned in Chap. 3, footnote 35. See also and compare with term 37.02.06 ISO Vocabulary for Biometrics 2012.

[182] About the various ways to circumvent a biometric system, see *below*, Part II, Chap. 4, §§ 92–116.

[183] JRC, Biometrics at the Frontiers, 2005, p. 56.

[184] See, e.g., JRC, Biometrics at the Frontiers, 2005, pp 44–45. It was reported at that time that for iris recognition, the enrolment process can be fairly long (30 s to 2–3 min) while no medical evidence has been reported so far although iris recognition has been used for some time.

140. On the other hand, diseases[185] or disabilities[186] may also affect the use of the biometric characteristic in a system. Another issue is hence *whether medical information may be derived from the biometric characteristics* but also the *inclusion/exclusion* and *discrimination* of particular person(s) who are not in the physical possibility to provide (good quality) characteristics. These important other aspects of the use of biometric data will be analyzed *below* in Part II, Chap. 4, while these aspects are to be distinguished from the concerns about the 'direct medical implications'.

2.2.4 Biometric Applications in the Public and Private Sector

141. Because of the considerable potential of the automated use of biometric characteristics and the promises of secure methods of identification and identity or other claim verification, biometric systems have been widely introduced in the public and in the private sector.

In the *public sector*, biometric systems are used by public authorities (in addition to law enforcement authorities) as a method for the verification of the authenticity of documents and of the identity of the holder (for example, of identity documents), and for identification purposes, the establishment of unique identities and double enrolment checks (for example, of asylum seekers or for nation wide ID schemes). Several of these systems have been set up at the level of the (European) Union. National initiatives are taken as well.[187] An important accelerator of the introduction of biometric systems was the call for the strengthening of the control at the external borders of the Union.[188] We see, however, that once such systems are set up, the purposes of border control, asylum and immigration control system have often been extended and that the data are used and become accessible for other purposes, such as for law enforcement. Some of these systems used by public authorities will hereunder be briefly described.

---

[185] For example, some reports refer to diseases such as glaucoma, diabetes or high blood pressure which may alter the patterns of the retina. See also Part II, Chap. 4.

[186] For example, the loss of a finger or hand.

[187] The largest national biometric program ever, addressing 1.2 billion people, using iris, finger and facial recognition, is currently being set up by the Indian government. See the Unique Identification Authority of India, Planning Commission, Government of India, available at http://uidai.gov.in/; see also G. Greenleaf, 'India's national ID system: Danger grows in a privacy vacuum', *Computer Law & Security Review*, 2010, pp. 479–491.

[188] This was needed due to the abolishment in 1995 of the internal borders of the signatory states of the Schengen Agreement, being replaced by one single external border. This required further cooperation with regard to visas, asylum requests and border controls. Furthermore, cooperation and coordination between police and judicial authorities has been strengthened within the Schengen area. The Treaty of Amsterdam of 1997 effectuated the incorporation of the Schengen cooperation into the Union legal framework. One should note that not all European Union Member States participate in the Schengen area and the Schengen acquis (i.e. the whole of legal regulations of the Schengen cooperation).

At the *same time*, *law enforcement authorities* start to use more extensively automated fingerprinting systems and are relying increasingly on automated biometric databases, in particular of fingerprint,[189] often in cooperation with law enforcement authorities in other countries.

In the *private sector*, the deployment of biometric systems varies from the use for increasing the security of access control to places, networks and information, over the use for administrative purpose and for convenience reasons. In some cases, private sector entities cooperate with public authorities. Government regulation, requiring enhanced security and strong user authentication for accessing particular (online) information (for example, in the healthcare or financial sector), does not yet play a major role in the adoption of biometric systems.[190] Exact information about the dispersion of biometric systems in the private sector however remains difficult to obtain.

2.2.4.1 Large-Scale Use of Biometric Systems in the Public Sector

142. Large-scale biometric systems have been introduced and are used in the public sector on a national and international level. *Multi-annual programmes* and *policies* developed in the Union have had a great influence in the set up and in the operation of these system.[191] Furthermore, several initiatives were taken and structural (re-) organizations were accomplished to increase the information exchange (which information will now also include biometric data) among law enforcement authorities.[192] New principles, such as the principle of availability in law enforcement matters,[193] put further pressure on these systems to expand.

We will hereunder give a brief description of some selected systems, in particular recently established large-scale systems set up in the Union. Our legal analysis later in this work will refer to some of these biometric systems as an example because the experiences with and the developments of these existing systems are useful for the further discussion on biometric data processing. Some of the systems mentioned however touch or belong to the domain of law enforcement,

---

[189] The biometric characteristics used in this field, however are being extended, and will include many more characteristics, e.g., palm prints.

[190] However, regulations on health and meals in schools may supposedly have influenced the use of biometric systems for meal registration in some countries, such as Scotland.

[191] E.g., the 'The Hague Programme' (see *below* at § 145).

[192] Besides several new initiatives (see, e.g., European Commission, *Commission Working Document on the feasibility of an index of third-country nationals convicted in the European Union*, COM(2006) 359 final, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0359:FIN:EN:HTML), existing organizations aim to improve the information exchange, *inter alia* by adding biometric identifiers (see, e.g., Europol, the Prüm cooperation, … as discussed *below*).

[193] This principle requires that if particular law enforcement information is available in one Member State it should also be available to authorities with equivalent competences of other Member States or Europol. For a discussion of this principle, see Part II.

which is not in the scope of our research. On the other hand, the existence of such databases cannot be neglected in the research of legal aspects of biometric data processing. The order in which the systems are discussed is more or less chronological. An overview of existing large-scale systems and the individuals affected thereby, is given in Table 2.3 *below*.

2.2.4.1.1 Europe

Eurodac: A Fingerprint Database of Asylum Seekers and Aliens

143. Eurodac (*Euro*pean *Dac*tylographic System) is a *central fingerprint database* and the first large-scale automated fingerprint identification system in the Union. The system has been set up since 2000.[194] It was aimed to determine which Member State is responsible for examining an asylum application lodged by a third-country national in one of the Member States pursuant to the Dublin Convention.[195] The system was intended to speed up the asylum procedure.

The database is established on the basis of Council regulation (EC) 2725/2000 adopted in December 2000 ('Eurodac Regulation 2000')[196] and became operational in 2003. It contains all *ten fingerprints* of every asylum applicant and alien apprehended for irregular border crossing or found illegally present in a Member State over 14 years old. These prints are taken and are together with other data, such as place and date of the asylum application, the Member State of Origin, gender and a reference number transmitted by the Member State to the system. Eurodac operates using the Automated Fingerprint Identification System (AFIS).[197]

---

[194] Before Eurodac was set up, Member States used national systems to check whether asylum seekers had applied for asylum under other names. In Belgium, for example, the Ministry of the Interior, Foreigners' Affairs, used the Printrak system since 1993 for these purposes. See W. Van de Voorde, J. Goethals en M. Nieuwdorp (eds.), *Multidisciplinair forensisch onderzoek*, Brussel, Politeia, 2003, p. 321 ('Van de Voorde, Goethals, Nieuwdorp, Multidisciplinair forensisch onderzoek, 2003').

[195] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, – Dublin Convention, signed in Dublin on 15.06.1990, *O.J.* C 254, 19.08.1997, pp. 1–12 ('Dublin Convention 1990'). The Dublin Convention 1990 contained almost identical provisions concerning asylum applications and the responsibility of Member States as set forth in the Convention implementing the Schengen Agreement (see *below*) which created a single external border where immigration checks would be carried out. The Dublin Convention 1990 has been replaced by the Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, *O.J.* L 50, 25.02.2003, pp. 1–10 ('Dublin II Regulation 2003').

[196] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *O.J.* L 316, 15.12.2000, pp. 1–10 ('Eurodac Regulation 2000'); see also Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000, *O.J.* L 62, 5.03.2002, pp. 1–5 and the implementing Commission Regulation (EC) No 1560/2003 of 2 September 2003, *O.J.* L 222, 5.09.2003, pp. 3–23.

[197] About AFIS, see *below* § 164.

The fingerprints are accessible via the Central Unit established within the EU Commission which operates the central database on behalf of the Member States. The purpose of the processing is the facilitation of the implementation of the Dublin Convention 19990, in particular the information exchange. This information may only be used 'as is necessary for determining the Member State which is responsible for examining the application for asylum, examining the application for asylum' and 'implementing any obligation arising under this Convention' (Article 15(1) Dublin Convention). The Eurodac Regulation 2000 and the Council Regulation (EC) No 407/2002 of 28 February 2002 contain the specific rules on the transmission of the fingerprints, the comparison, the transmission of the results, data use and data protection. In the meantime, there have been several Commission Proposals and Amended Proposals for adapting the Eurodac Regulation 2000, the latest of May 2012, requesting comparisons with Eurodac by Member States' law enforcement authorities and Europol for law enforcement purposes, which has been amended again (see also Part II, Chap. 4, § 186).

144. The objective of Eurodac is to allow for the *identification* of *asylum seekers*. These persons often arrive without any documents. The collected biometric data and the mode of comparison (1:n) are deployed for attaching an identity to the individual. The system also permits an examination for *double requests* among asylum seekers' applications that were lodged with different Member States. Upon recording of the transmitted fingerprints in the central database, the Central Unit enables the comparison of the fingerprints with those already stored in the database. In case of a 'hit', data will be sent back to the transmitting Member State for comparison and than a final identification decision will be made in cooperation with the Member States.[198] Eurodac also allows for the cross-checking of fingerprints of *aliens* apprehended in connection with *irregular crossing* of an external border or found *illegally present* in a Member State.[199]

[198] See Article 4.6 of the Eurodac regulation 2000. In particular, in case a comparison of fingerprints provides positive results, additional data, such as name and picture, is exchanged The name, date of birth, the nationality and other identifying information is in principle not mentioned with the fingerprint in the database as a protection against possible misuse of data in the database.

[199] For aliens apprehended in connection with irregular crossing, the data, including the fingerprint data, will only be recorded for comparing with asylum application data (see Articles 8–10 Eurodac Regulation 2000). Member States may also transmit fingerprint data of aliens found illegally on the territory of a Member State. These data however shall not be centrally stored and only be compared with asylum application data (see Article 11 Eurodac Regulation 2000). With the term 'cross-checking', reference is in fact made to a 1:n search (identification functionality). About Eurodac, see D. Broeders, 'Mobiliteit en surveillance: een migratiemachine in de maak', in H. Dijstelbloem and A. Meijer (eds.), *De Migratiemachine*, Serie kennis, openbare mening, politiek, Amsterdam, Rathenau Instituut/Van Gennep, 2009, (35) pp. 48–51 ('Broeders, Mobiliteit en surveillance, in Dijstelbloem and Meijer, De Migratiemachine, 2009'); E. Guild, 'Chapter IV. Unreadable Papers ? The EU's first experiences with biometrics: Examining EURODAC and the EU's Borders', in J. Lodge (ed.), *Are you who you say you are* ? *The EU ad Biometric Borders*, Nijmegen, Wolf Legal Publishers, 2007, pp. 31–43.

Biometric Identifiers in Passports and Travel Documents

145. One of the ten priorities outlined in the so-called The Hague Programme adopted at the European Council meeting of 2004[200] was to make identification and travel *documents* more *secure* by equipping them with *biometric identifiers*. Another priority outlined in the The Hague Programme was the creation of an effective visa policy.

146. Regulation No 2252/2004 was passed in 2004 in the Union for the purposes of harmonizing the security standards and the use of biometrics for passports and travel documents.[201] Member States *must* introduce for this purpose facial images ànd fingerprints in the electronic storage medium of new passports ('biometric ePassport').[202] Article 4 states that the purpose of the use of the biometric characteristics in such passports is (only) 'for *verifying* (a) the *authenticity* of the document' and '(b) 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*' (emphasis added).

Regulation No 2252/2004 also ensured that the EU Member States meet the requirements of the US Visa Waiver Program.[203]

147. Regulation No 2252/2004 has been amended by Regulation No 444/2009.[204] Particular groups of people have been exempted from having to provide fingerprints, in particular children under the age of 12 and persons where fingerprinting is physically impossible. Qualified and duly authorized staff shall take the biometric identifiers (new article 1a). Fall back procedures have been stipulated in case it is temporarily impossible to fingerprint any of the fingers. The Regulation also requires from the Commission before June 2012 a 'large scale and in-depth study' which examines the reliability and the technical feasibility' including through an 'evaluation of the accuracy of the systems in operation' of fingerprint of children under 12 'for identification and verification purposes' (new Article 5a). This study

---

[200] The Hague Programme was adopted at the European Council (the heads of State and government of the Member States of the European Union) meeting of 4 and 5 November 2004. It set out ten priorities for the next 5 years for the European Union with a view of strengthening the area of freedom, security and justice, including for border control, border management and border surveillance. European Commission, *Communication of 10 May 2005 from the Commission to the Council and the European Parliament – The Hague Programme*: *Ten priorities for the next 5 years. The Partnership for European renewal in the field of Freedom*, *Security and Justice*, COM(2005) 184 final ('The Hague Programme, 2005').

[201] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 385, 29 December 2004, pp. 1–6 ('Regulation No 2252/2004' or 'ePassport Regulation'); see also the many critical comments of the Article 29 Data Protection Working Party on the ePassport Regulation in its opinion WP112 adopted on 30.09.2005.

[202] Article 1 (2) of Regulation No 2252/2004.

[203] See *below* at § 165.

[204] Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 142, 06.06.2009, pp. 1–4 ('Regulation No 444/2009' or 'Amended ePassport Regulation 2009').

however was delayed and now announced for mid-2013. In 2012, the biometric ePassport was debated in the European parliament and several questions were asked.

Visa and VIS

148. The the Hague Programme also mentioned the development and use of a Visa Information System as an example to reach an effective visa policy. The set up of such system was considered a first step towards a future European common consular service.

149. The Council of Ministers of the Union decided in June 2004 to establish a Visa Information System ('VIS').[205] The Council provided hereby the legal basis for the invitations for tenders for this system which were already under way and for the inclusion of the costs in the general budget of the EU. According to the Decision of 2004, VIS is an information system intended to enable authorized national authorities to *enter and update visa data* of *third country nationals* and to *consult* these data electronically (Article 1). VIS was generally intended (a) to improve the consular cooperation and consultation amongst the central consular authorities, (b) to improve the administration of the common visa policy and (c) to prevent 'visa shopping'. The Decision needed further implementation at the Union and the national level.

150. Regulation No 767/2008 of 9 July 2008 provides the further implementation ('VIS Regulation 2008').[206] The VIS Regulation 2008 sets up the conditions and procedures for the *exchange of data* between Member States on applications for short-stay visas and on the decisions taken in relation thereto. Personal data of third country nationals to be recorded in the *central database* of VIS include not only a list of alphanumeric data, such as surname and first name, but also *photographs and fingerprint data* (Article 5 1. (a), (b), (c) of the VIS Regulation 2008). The biometric data were hence principally aimed to allow to verify whether the third country national, to whom the visum has been issued in a third country, is actually the same person entering the Union with that visum after verification with the data stored at the issuance of the visum. While the initial purpose of VIS was to *improve the common visa policy*, *consular cooperation and consultation*

[205] Council Decision of 8 June 2004 establishing the Visa Information System (VIS), 2004/512/EC, *O.J.* L. 213, 15.06.2004, pp. 5–7. This decision was taken after a so-called 'extended impact assessment' submitted by the Commission to the public. See European Commission, JHA, *Your views on the future EU Visa Information System* (*VIS*), available at http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_vis_en.htm. This public consultation was decided by the Commission in its Annual Work Program 2004.

[206] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, *O.J.* L 218, 13.08.2008, pp. 60–81 ('VIS Regulation 2008'). The regulation was subject to the procedure of co-decision. About the draft Regulation, see M. Meints, and M. Hansen, (eds.), *D.3.6 Study on ID Documents*, Frankfurt, FIDIS, December 2006, pp. 45–49 ('Meints and Hansen, Study on ID Documents, Fidis, D.3.6, 2006').

by facilitating the exchange of data (see Article 1 of the VIS Decision of 2004), the VIS Regulation 2008 however now also mentions other purposes such as *inter alia* the *fight against fraud*, *checks* at external borders or otherwise, *identification* of illegal immigrants and the prevention of *threats to the internal security* (see Article 2). In addition, the data are made *available* for the prevention, detection or investigation of *terrorist* offences and of other *serious criminal offences*. Article 3 states that 'designated authorities (…) may in a specific case and *following a reasoned written or electronic request* access the data kept in the VIS (…) if there are *reasonable grounds* to consider that consultation of VIS data will *substantially contribute* to the prevention, detection or investigation of terrorist offences and of other serious criminal offences'. The access by 'designated authorities' of Member States and Europol to VIS for purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences was confirmed in the decision of the Council of 23 June 2008.[207] The (biometric) data contained are hence used for both – as what was previously known – First and Third Pillar matters,[208] while the privacy and data protection rules for the processing of information in these pillars differ considerably.

We should hence retain that while VIS was set up in 2004 to improve the implementation of the common visa policy of the Union, hereby aiming at providing border guards all necessary information to verify whether the entry conditions for third country nationals are fulfilled at the external borders, this purpose has been considerably extended in 2008.[209]

151. The VIS Regulation 2008 also contains specific provisions relating to the *access* to the data by the competent authorities and the *search criteria*. Because of the additional purposes, not only authorized staff of visa authorities are entitled to use the data and have access thereto (articles 15 and 16). Also *other authorities* that are competent for activities beyond a common visa policy have access to the biometric data. According to the VIS Regulation 2008, such other competent authorities (at the borders and within the national territory) have access to a search facility *using the number* of the visa sticker *in combination with the verification of fingerprints*[210] of the visa holder for purposes of *verifying* (1:1 comparison) the

[207] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *O.J.* L. 218, 13.08.2008, pp. 129–136 ('VIS access Decision 2008').

[208] About the three-pillar structure introduced by the Maastricht Treaty (and which has in the meantime been abolished by the Lisbon Treaty), see Chap. 3, § 395.

[209] One should note that the recitals to the Decision of 2004 mentioned the option of a common technical platform with the second generation Schengen Information System (SIS II, see *below*) (recital 2). This common platform is supposedly the so called Biometric Matching System (BMS), which will be used in *inter alia* VIS and SIS II. About the 'function creep' of VIS, see also Part II, Chap. 4, § 185.

[210] All ten fingerprints (in accordance with the Common Consular Instructions) of applicants will be stored in the VIS central database located in Strasbourg (and not in the visa sticker as initially envisaged).

identity of the visa holder and/or the authenticity of the visa and/or as to whether the conditions for entering the Schengen area or the stay on the territory are fulfilled (Article 18 and 19). Access to 'other authorities' for *identification purposes* (1:n check) whereby *the use of the biometric data is used as a search criterion* is also regulated and will be operational (Article 20), as well as access for determining responsibility for asylum applications (Article 21).[211]

In the long term, it is expected that VIS will be one of the largest biometric databases in Europe.[212] The entry into operation and gradual roll out of VIS however was postponed and last scheduled for June 2011.

152. It is further remarkable that only 6 months after VIS Regulation 2008 a new Regulation (EC) No 81/2009 of 14 January 2009 already provides for a derogation to the use of the biometric data in the central database of VIS when the waiting lines are too long. In Regulation (EC) No 81/2009, it is stated that '*where traffic of such intensity arises that the waiting time at the border crossing point becomes excessive*, *all staff and facilities resources have been exhausted and based on an assessment there is no risk related to internal security and illegal immigration*, *VIS may be consulted using the visa sticker number only*, *leaving out the verification of fingerprints* (Article 1.1(ab))'.[213]

SIS and SIS II

153. In 1995, the Convention implementing the Schengen Agreement abolished the internal borders of the Schengen signatory States.[214] Following the creation of the Schengen area, the Schengen Information System ('SIS') was set up to allow competent authorities in the Schengen Member States to facilitate *information*

[211] VIS will also allow competent asylum authorities to search with the fingerprints of the asylum seeker and will hence also assist in the identification and return of illegal immigrants facilitating the application of the 'Dublin II Regulation' (EC) No 343/2003.

[212] It is envisaged that VIS will contain visa data of about 70 million people. See CNIL, *Système d'information sur les visas VIS*: *dernières négociations avant la mise en oeuvre de la plus grosse bse d'empreintes digitales au monde*, 22.08.2006, p. 1. The VIS roll out is on a regional basis and started in late 2011 in particular north African countries (see Commission Decision of 30.11.2009).

[213] Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Border Code, *O.J.* L 35, 4.02.2009, pp. 56–58 ('Regulation No 81/2009 amending VIS').

[214] Convention applying the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at their Common Borders, 19 June 1990, as amended ('1990 Schengen Convention'). The Convention came into effect in 1995. Many countries have joined the Schengen agreement and co-operation. In 1997, the 'Schengen Acquis' was incorporated in European Union law through the Amsterdam Treaty. The 'Schengen Acquis' is formed by the legal documents forming the Schengen body of rules and regulations. About these developments, see e.g., S. Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*, Leiden, Martinus Nijhoff, 2008, pp. 26–27 ('Karanja, Transparency and Proportionality in SIS and Border Control Co-operation, 2008').

exchange.[215] The creation of the Schengen area implied that there was a political consensus that the security at the external borders needed to be enhanced against *illegal immigrants* and internally against *criminals*. SIS, which is operational since March 1995, is used on the national territories for external border control (immigration), for the issuance of visa and residence permits, and in the context of police-cooperation, security and judicial cooperation in criminal matters, for example, to obtain information about persons and objects (e.g., a vehicle) which are signaled[216] or to transmit a European arrest warrant.[217] The requests are automated. SIS covers both what was previously known as First and Third Pillar matters, but does *not* contain biometric data.

154. The Second Generation Schengen Information System, commonly referred to as SIS II, however, allows for the *central* storage of biometric data (fingerprint and photographs) on persons in relation to whom an alert has been issued and widens access to the information contained therein as compared to SIS. Three different instruments were necessary for SIS II in order to be based on the correct legal basis.[218] SIS II allows *inter alia* alerts to be inter-linked, biometric data to be transferred and access is foreseen to new authorities (e.g., Europol, Eurojust,[219]

[215] About SIS and data protection, see also J. Dumortier, 'Het Schengen Informatie Systeem en de bescherming van persoonsgegevens', in C. Fijnaut, J. Stuyck, and P. Wytinck (eds.), *Schengen*: *Proeftuin voor de Europese Gemeenschap* ?, Antwerpen, Kluwer, 1992, pp. 119–173.

[216] There are a number of categories of 'alerts' defined in the 1990 Schengen Convention. 'Alert' is used in a technical sense, and is defined (in SIS II) as 'a set of data entered in SIS II allowing the competent authorities to identify a person with a view to taking specific action'.

[217] Article 95 of the 1990 Schengen Convention.

[218] These were related to Union immigration law powers, transport law powers (for access to data on stolen vehicles) and policing and criminal law powers: Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, *O.J.* 2006 L381, 28.12.2006, pp. 1–3 ('SIS II Regulation Access Vehicle Registration Services'), Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *O.J.* 2006 L381, 28.12.2006, pp. 4–23 ('SIS II Regulation') and the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the Second Generation Schengen Information System (SIS II), *O.J.* L 205, 7.08.2007, pp. 63–84 ('SIS II Decision'). See also about the development of SIS II, Council Regulation (EC) No 2424/2001 of 6.12.2001 as amended by 1988/2006 of 21.12.2006 and Council Decision 2001/886/JHA of 6.12.2001 as amended by Council Decision 2006/1007/JHA. See further also the Council Regulation (EC) No 1104/2008 and Council Decision 2008/839/JHA of 24 October 2008, referred to as "the migration instruments" for the migration from SIS I to SIS II, and which relate *inter alia* to comprehensive testing of the system.

[219] Eurojust is a new European Union body aimed at enhancing the effectiveness and the coordination of investigations and prosecutions of serious cross-border and organized crimes by the national authorities of Member States. It was set up in 2002 and operational since 2004. The implementation of extradition requests and international mutual legal assistance is at the core of its activities.

national prosecutors, vehicle licensing authorities), where necessary, for purposes other than those originally laid down. In the meantime, more countries have joined the Schengen agreement and co-operation, and therefore also obtained access to SIS II (for example, at the end of 2008, Switzerland). Central search facilities are on an individuals' name. The biometric data will not be used as a search criterion, but in principle only to confirm the identity of a third-country national (Article 22 (b) SIS II Decision). Furthermore, the SIS II legislation permits the use of *one-to-many searches only* once the Commission reports that the relevant *technology is available and ready* (Article 22 (c) SIS II Decision).[220] So far, there have been various delays in the development of SIS II. The entry into operation is now foreseen for 2013, depending on the technical solution followed.[221]

Prüm Cooperation amongst Police and Law Enforcement Agencies

155. In 2005, the Treaty signed in Prüm between Austria, Belgium, the Netherlands, France, Germany, Luxembourg, and Spain on international police co-operation has introduced far reaching measures on the improvement of *cross-border* information *exchange* and data *comparison*, in particular of fingerprints, DNA profiles and vehicle registration data.[222]

156. The provisions of the Prüm Treaty provide for reciprocal access rights to national information systems (databases) containing DNA analysis files (see articles 2–7), to automated dactyloscopic identification systems (see articles 8–11) and vehicle number-plates (see article 12). By Council Decisions 2008/615/JHA and 2008/616/JHA, essential parts of the Prüm Treaty have been *integrated* in the legal framework of the Union. Member States have to comply with the Prüm provisions which have become binding European law within a specific timeframe. These Decisions providing inter alia *online access to other Member States' national databases* are seen as a very important step in view of the implementation of the

[220] It is stated that as soon as it 'becomes technically possible, fingerprints may also be used to identify a third-country national on the basis of his biometric identifier' ((Art. 22 c) SIS II Regulation). The involvement of the European Parliament, in particular the LIBE committee, in the adoption of the SIS II legislation, has been important.

[221] See also the dates set forth in the Commission's Action Plan Implementing the Stockholm Programme (about this Programme, see Part III, Chap. 7, § 18 and footnote 38).

[222] Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, Prüm, 27 May 2005, Council Secretariat, Brussels, 7 July 2005, 10900/05 ('Prüm Treaty').

principle of availability.[223] Rather than establishing a (new) central database on Union level, the system provides online access to national AFIS databases and central DNA databases, including reference data but not from which the data subject can be directly identified (see Articles 2 and 8 Decision 2008/615/JHA), allowing for example for automated searches on a hit/no hit basis, as developed on the basis of the prototype developed by some initial signatory States of the Prüm Treaty (e.g., Germany, the Netherlands, …).

Europol-Information System

157. The Europol[224]-information system aims at centralizing all information that the EU Member States have about *organized crime* for which Europol is competent.[225] Information such as about the identity of suspects or convicts of criminal offences for which Europol is competent, *physical characteristics*, *fingerprints*, the *DNA profile* are registered in a central database.

158. The software for the database is available since 10 October 2005. Each Member State is responsible to feed the database and the database itself is

[223] See the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, as implemented by Council Decision 2008/616/JHA of 23 June 2008, both published in *O.J.* L. 210, 6.08.2008, pp. 1–72. The Decisions include very detailed provisions for the sharing by police of fingerprints, DNA data and vehicle registrations. By these Decisions, all Member States shall adopt the provisions of the Treaty, including on on-line access to and follow-up request relating to DNA profiles, fingerprint data and vehicle registration data. About making DNA information available, see also *Vr. & Antw.* Senaat 2010–11, 12 July 2011 (Question no 5-2691 of 12 July 2011 of Khattabi). On the principle of availability, see also *below* and Part III.

[224] The European Police Office, known as Europol, was set up by the Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office, as amended. Europol became operational in 1999, when it replaced the Europol Drugs Unit. Europol is established in The Hague. Its tasks are to facilitate the exchanges of information, analyze intelligence and coordinate operations involving several Member States. In general, its objective is to improve police cooperation between Member States in order to combat terrorism, unlawful drug trafficking and other serious forms of international organized crime. About Europol and its database(s), see also L. De Vlieger and N. Verstuyft, 'Politieregisters en privacy', in *Privacy en Strafrecht. Nieuwe en grensoverschrijdende verkenningen*, G. Vermeulen (ed.), Antwerpen, Maklu, 2007, (219), p. 250 *et seq.* ('De Vlieger and Verstuyft, Politieregisters en privacy, in G. Vermeulen (ed.), Privacy en Strafrecht, 2007'). As of 1 January 2010, the Europol Convention has been replaced by Council Decision 2009/371/JHA establishing Europol. Europol is now a Union entity. Europol shall not be confused with Interpol, which is an global international organization of police forces (not restricted to Europe), and which has an own system and database, the Interpol Criminal Intelligence Database (ICIS). See on ICIS and the interconnections with SIS, Karanja, Transparency and Proportionality in SIS and Border Control Co-operation, 2008, pp. 259–265.

[225] The forms of international crime for which Europol has a mandate are extended from time to time, and include for example also motor vehicle crime, counterfeiting and forgery of means of payment and money laundering.

controlled by the respective national Europol-service of each Member State.[226] In 2008, Europol has also obtained access to VIS (see *above*).

A European Border Surveillance System, Frontex, a European Union Registered Traveler Programme and an Entry/Exit System

159. In 2008, the EU Commission started a discussion on the next steps on border management, the creation of a European Border Surveillance System and the evaluation of Frontex. Frontex was set up in 2004 as a European agency for the management of the operational cooperation of the Member States at the external borders.[227] The agency is involved in the organization of joint return operations by Member States, but also carries out coordination of intelligence-driven operations based on risk analysis and threat assessment.[228] In December 2011, the EU Commission adopted a proposal for Regulation for establishing the European Border Surveillance System (EUROSUR), a common framework for reinforcement of the control at the Schengen external borders and the exchange of information and cooperation between the Member States and Frontex.[229]

160. The Article 29 Working Party, together with the Working Party on Police and Justice ('WPPJ') declared in 2008 that they make serious reservations as to the necessity and the proportionality of the proposals for the set up of the European Border Surveillance System and Frontex. They stated in a declaration that they regret that it is *not evaluated* first whether existing legal measures are properly implemented and proved to be inefficient which is needed to motivate the need for new systems. The inclusion of biometric data increases those risks. The WPPJ hereby interestingly underlined that 'not everything that is technically feasible is also ethically acceptable or legally permissible'.[230]

---

[226] About Europol and the system, see *Europol*: *European Police Office*, available at http://europa.eu/agencies/regulatory_agencies_bodies/pol_agencies/europol/index_en.htm

[227] Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, *O.J.* L 349, 25.11.2004, pp. 1–11. Council Regulation (EC) No 2007/2004 was amended by Regulation (EU) No 1168/2011, *O.J.* L 304, 22.11.2011, pp. 1–17.

[228] For a critical analysis of Frontex, see S. Carrera, 'Chapter VI. Frontex and the EU's Integrated Border Management Strategy', in J. Lodge (ed.), *Are you who you say you are* ? *The EU ad Biometric Borders*, Nijmegen, Wolf Legal Publishers, 2007, pp. 31–43.

[229] See European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (*EUROSUR*), COM (2011) 873final, 12.12.2011, 44 p.; see also COM (2008) 69 final, COM (2008) 68 final and COM (2008) 67 final.

[230] European Data Protection Authorities, Declaration adopted on the Spring Conference of European Data Protection Authorities, Rome, 17–18.04.2008, available at https://www.ip-rs.si/index.php?id=272&tx_ttnews%5Btt_news%5D=367&cHash=47956ed169f8c49b72d2a7cbe042d9d4. In May 2012, it was decided that the mandate of the WPPJ was not to be prolonged because of overlap of the activities with those of other bodies, such as of the Article 29 Working Party. From our further analysis, it will also become clear that, based upon an obligation to review whether the processing is not excessive, it is critical to first evaluate previous biometric data processing initiatives before starting new ones and to avoid an overlap between systems.

It is expected that the Commission will make further progress in establishing an interoperable EU Registered Traveler Programme (RTP), arguably to facilitate border crossing but whereby border control resources would be re-organized as well. The Commission also announced a legislative proposal to set up an Entry Exit System (EES) for the electronic recording of the place and the time of entry and exit by third country nationals of the Union, allowing for a calculation of authorized stays, as well as verification and identification of travelers. The RTP and EES, both planned to include biometric identifiers, would be the building blocks for setting up so-called 'smart borders'.[231]

Public Sector Use of Biometric Data is Gradually Expanding

161. An important aspect of the fore mentioned biometric applications in the Union, is the fact that the processing of biometric data for purposes other than law enforcement has been introduced in the public sector step by step, *first vis-à-vis non-EU citizens* (e.g., asylum seekers in Eurodac) and *third country nationals* (e.g., visum applicants in VIS), later by expanding the collection and use of biometric data from EU citizens applying for passports. In several Member States, decisions have been taken or discussions are going on about introducing biometric characteristics in the national electronic identity card ('eID').[232] An overview of the individuals, other than criminals, affected by some important large-scale biometric applications set up or being discussed in the Union, is given in Table 2.3 *below*.

For the moment, it is in our view not for all systems fully clear whether they affect all individuals mentioned *below*. It should further be noted that access to the biometric data collected for these applications has often been granted for law enforcement purposes (e.g., to VIS), or is under discussion.

---

[231] See European Commission, Communication from the Commission to the European Parliament and the Council, Smart borders – options and the way ahead, COM (2011) 680 final, 25.10.2011, 14 p. ('Commission, Smart borders COM (2011) 680 final'); see also EU Commission, *Management Plan 2011. DG Home*, 33 p., available at http://ec.europa.eu/atwork/synthesis/amp/doc/home_mp.pdf; R. Rinkens, *EU Large Scale IT Systems & Schengen RTP*, slide 8, 9.12.2010, presentation at Rise and Hide Conference, Brussels, 9–10.12.2010, previously available at http://www.riseproject.eu/_fileupload/RISE%20Conference/Presentations/Richard%20Rinkens.pdf; see also: *Roadmap for the Smart borders initiative*, 5 p., available at http://ec.europa.eu/governance/impact/planned_ia/docs/2010_home_004_entry_exit_system_2012_en.pdf; for a critical report about these initiatives, see B. Hays, and M. Vermeulen, *Borderline. The EU's New Border Surveillance Initiatives. Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, Heinrich Böll Foundation, June 2012, 82 p., available at http://www.statewatch.org/news/2012/jun/borderline.pdf ('Hays and Vermeulen, Borderline, 2012'); about the PNR proposal, see Part II, Chap. 5, footnote 344.

[232] For an overview of 2005 on the introduction or the debate about biometric data in eIDs in particular countries, see, e.g., LSE, Identity Project, 2005, pp. 65–78; about the discussion in France and for a recent overview of (biometric) eIDs in Europe, see CNIL, *32 ième Rapport d'Activité 2011*, Paris, La Documentation française, 2011, pp. 46–49 ('CNIL, 32 ième Rapport d'Activité 2011').

Table 2.3 Overview of some large-scale (biometric) applications in the Union for public sector use and categories of individuals affected

Asylum seekers	Third country nationals	EU citizens	All nationals of EU Member States ?
Eurodac	Eurodac	Biometric ePassports ((Regulation (EC) 2252/2004)	Biometric eIDs
		(EU citizens applying for passport or crossing Union borders)	
	VIS	VIS (if sponsor of visa applicant)	VIS (if sponsor of visa applicant)
Frontex information system	Frontex information system	Frontex information system?	Frontex information system?
Prüm information cooperation	Prüm information cooperation	Prüm information cooperation	Prüm information cooperation
SIS II check	SIS II check	SIS II check	SIS II check
	Smart borders initiatives (planned RTP and entry exit system)	Smart borders initiatives (planned RTP system)	Smart borders initiatives (planned RTP system)

2.2.4.1.2 The International Civil Aviation Organization (ICAO)

162. In 1999, an advisory group within the International Civil Aviation Organization (ICAO) initiated a study for quantifying the compatibility of available biometric techniques for adoption in Machine Readable Travel Documents (MRTDs). In 2003, ICAO selected the *facial image* and *facial recognition* as the globally interoperable 'biometric' for Machine Readable Travel Documents ('MRTDs'), such as passports.[233] Fingerprint and iris recognition may be added by issuers.

163. Since the adoption by the Council of the European Union of the Regulation on mandatory *facial images* ànd *fingerprints* in ePassports in 2004, many European countries started to issue passports which include biometric identifiers in a microprocessor chip ('biometric ePassports'). The introduction of these biometric

[233] See in particular ICAO, Document 9303 on machine readable travel documents, consisting of 3 parts (see, in particular, Part 1, Machine Readable Passports, Volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format, 6th edition, 2006, 99 p. available at http://www.icao.int/publications/Documents/9303_p1_v1_cons_en.pdf and Part 1, Machine Readable Passports, Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability, 6th edition, 2006, 131 p. available at http://www2.icao.int/en/MRTD/Downloads/Doc%209303/Doc%209303%20English/Doc%209303%20Part%201%20Vol%202.pdf containing the document and chip specifications for the biometric ePassport). ICAO specifications, when endorsed by ISO (see *below*), may also become ISO standards.

ePassports has been much debated in many countries, in particular because of weak security aspects and the Member States' decisions about the place of storage of the biometric data. The biometric ePassport will – as a specific case illustrating some arguments made relating to the use of biometric data – be further analyzed *below* in Part III.[234]

2.2.4.1.3 The United States

164. In 1999, a large-scale *ten-fingerprint* identification system of the FBI and database, known as IAFIS (Integrated Automated Fingerprint Identification System), became operational.[235] About 20 years before, the Automated Fingerprint Identification System, better known as AFIS, was started up by law enforcement authorities, including in the United States, and since then AFIS has been used in many countries. AFIS allows to search latent fingerprints found at crime scenes against a collection of fingerprint files. AFIS is part of IAFIS. However, fingerprint is just one type of biometric characteristic used for criminal investigations. In 2008, the Federal Bureau of Investigation engaged a contractor to set up a 1 billion U.S.$ vast database with several other types of biometric characteristics, including iris and facial images, as well as DNA and DNA samples.[236]

165. In 2002, shortly after the events of September 2001, the Enhanced Border Security and Visa Entry Reform Act was passed.[237] The Act mandated to include biometric data in the passports of VISA Waiver Program travelers (e.g., Belgian nationals as well as many other Union Member State citizens).[238]

In 2004, the *U.S. Visitor and Immigrant Status Indicator Technology* (*US-VISIT*) *program* was set up for checking biometric data of foreigners. US-VISIT is an automated entry-exit system to increase security and is in use. For visitors requiring a visa, fingerprints and digital photographs are taken at the US visa issuing posts, later compared with those of the persons crossing the U.S. border. For Visa Waiver travelers admitted without a visa, a machine-readable passport is needed, and, upon entrance in the United States, as well as submission of (initially) two digital index

[234] About the biometric ePassport, see further in more detail Part III, Chap. 7, §§ 179–189, as well as the several references throughout this work. It shall be noted that the biometric ePassport leads on its turn to plans and discussions about the adoption of national biometric eIDs.

[235] See also NSTC, Biometrics History, 2006, p. 18.

[236] See on this project, e.g., CNN, FBI Biometric Database Plan, CNN News Report, 12.02.2008, available at http://www.youtube.com/watch?v=jADItDHOHOA

[237] The Act was further based on the U.S.A. Patriot Act (H.R. 3162), which required additional regulations and *inter alia* the development of 'a technology standard that can be used to verify the identity of persons applying for a visa or such persons seeking to enter the United States pursuant to a visa for purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name (…)' (see, e.g., section 403 (c)).

[238] Enhanced Border Security and Visa Entry Reform Act 2002, Pub. L No. 107–173 (H.R. 3525), section 303.

finger scans and a digital photograph, later increased to ten fingerprint scans in late October 2008.[239] The objective is *to know as much as possible* about *every non-U.S. citizen* before allowing entrance to the country. The biometric data are compared against several databases for various purposes, including to know whether the traveler has been previously been determined as inadmissible, is in the FBI's IAFIS database, is on a watch list, or has previously overstayed the visa terms.[240] US-VISIT is reported to be used every day by 30,000 authorized federal, state and local government users.[241]

166. The United States government also called for biometric identifiers for example for use in a personal identification card for all federal employees and contractors requiring access to federal facilities and systems.[242]

167. Biometric systems are also used oversees. Media reported the use of mobile scanners by U.S. military troops in Iraq to capture *inter alia* fingerprints and eye scans from Iraqis.[243] The Department of Defense has also implemented an Automated Biometric Identification System (ABIS) to track and identify national security threats. The system allows to collect from enemy combatants, captured insurgents and other persons ten rolled fingerprints, face images, voice samples, iris images and oral swab to collect DNA.[244]

2.2.4.1.4 Other Countries and Organizations

168. The spread of the use of biometric data and automated biometric systems is not limited to the countries above. Malaysia, for example, was in 2001 one of the first countries to use biometric data, i.e., thumbprint, on its national ID card. The card is in fact a government multipurpose card, quickly becoming a *de facto* requirement to

---

[239] Reasons include likely the aim for increased accuracy but probably also comparison with the FBI standard ten-print records.

[240] On US-VISIT, see, e.g., JRC, Report Large-scale Biometrics Deployment 2008, pp. 63–64. For an overview of the U.S. agencies having access to US-VISIT, see Department of Home Security, *Government Agencies Using US-VISIT*, available at http://www.dhs.gov/files/programs/gc_1214422497220.shtm

[241] *Ibid*.

[242] This use was called for by a President Bush Homeland Security Presidential Directive 12 (HSPD-12) of 2004, available at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm; for the standard developed, see NIST, *Personal Identity Verification* (*PIV*) *of Federal Employees and Contractors*: *Federal Information Processing Standard* (*FIPS*) *201 approved by the Secretary of Commerce*, available at http://www.itl.nist.gov/lab/bulletns/bltnmar05.htm

[243] Electronic Privacy Information Center, *Iraqi Biometric Identification System*, available at http://epic.org/privacy/biometrics/iraq.html

[244] See Biometrics Task Force, Biometrics History. The Department of Home Security has further been developing in 2011 a shared biometric database allowing border agents access to the Department of Defense (DOD)'s biometric database. See X., DHS develops shared biometrics database with DOD, 8.03.2011, available at http://homelandsecuritynewswire.net/dhs-develops-shared-biometrics-database-dod

access certain government and private-sector services.[245] Australia initiated a strategy for identity management at the border which includes passports for Australian citizens enabled with chips allowing for biometric identifiers.[246] Biometric data have also been used in Canada, for example, for the organization of social welfare in case of unemployment but also as anti-terrorism measure. Some other countries use or have planned to use biometric data in governmental identity schemes (e.g., the United Kingdom),[247] but these plans, often announced widely, are sometimes changed. China, for example, moved in the direction of compulsory ID databases, but would have abandoned the biometric element after it concluded that the technology was unworkable with large populations.[248] India has recently started and will be implementing the so far largest governmental biometric identity scheme ever, collecting biometric data of its 1.2 billion citizens (see also § 141 *above*).

169. International organizations have also been active in the adoption of automated biometric methods. The International Labor Organization (ILO), for example, introduced compulsory biometric identifiers for seafarers.[249]

2.2.4.2 Deployment in the Private Sector

170. Biometric systems are increasingly used in the private sector as well. Beside some public discussion on the implementation of biometric systems, e.g., in schools,[250] the introduction of biometric systems in the private sector generally *goes more undocumented* and *without much debate* as compared with the use by public authorities. For the Netherlands, a research project attempted to draw up an inventory of small-scale biometric applications in use in the semi public and private sector, but it proved difficult to obtain and verify this information.[251] In other countries,

---

[245] Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments*, Washington – London, Electronic Privacy Information Center and Privacy International, 2007, p. 668. The card is termed 'MyKad'. It allows for its holders several 'electronic conveniences', ranging from health services to transportation. See also Malaysia National ICT Initiative, *More with MyKad. Your Lifestyle Programmed into One Card*, available at http://www.mscmalaysia.my/topic/More+with+MyKad

[246] See Australian Government, Department of Immigration and Citizenship, *Identity matters : Strategic Plan for Identity Management in DIAC 2007–2010*, Department of Immigration and Citizenship, Canberra, available at http://www.immi.gov.au/managing-australias-borders/border-security/systems/identity.htm#b

[247] On the plans to introduce a UK ID-scheme based on biometric data, and a critical review, see LSE, Identity Project, 2005.

[248] *Ibid*., p. 57. Another example is Taiwan. *Ibid*, p. 64. See also the decision of 2005 of the Taiwanese Constitutional Court, as mentioned in Part II, Chap. 4, footnote 80.

[249] The International Labor Organization (ILO) Convention No 108 was modified in 2003 for this purpose.

[250] See, e.g., in France, Belgium and the United Kingdom. See also Part III.

[251] See De Hert, P. and Sprokkereef, A., *The Use of Privacy Enhancing Aspects of Biometrics. Biometrics as a PET* (*privacy enhancing technology*) *in the Dutch private and semi-public domain*, Centrum voor Recht, Technologie en Samenleving, January 2009, p. 23 ('De Hert and Sprokkereef, Biometrics as a PET, 2009'). This report contains an overview of about 100 projects in the private and semi-private sector (see pp. 47–50).

for example Germany, biometric system producers have made a geographical map for allowing purchasers to find expert advice and to access product information in an effort to make product information accessible.[252] On the other hand, pilot projects which do get much attention in the press, mainly for commercial reasons, often are after the tests sometimes discontinued.

171. In the private sector, biometric systems are for example used for enhancing the *security* of logical or physical *access*. In many cases, *employers* install biometric applications for securing and controlling the access to their premises by their employees. Owners of *shops* or organizers of *public events* may also use biometric systems for access control or for surveillance with the aim to enhance public safety (e.g., at a football stadium).[253] Biometric systems are also used for *administrative* and *management* purposes, such as for time and attendance control of employees and meal registration of students.[254] The control of *identity*[255] or the control of *membership* of a club (e.g., a fitness club) are other aims of the use of biometric data in the private sector. Another well known example is the Privium membership card which is available for *frequent flyers* at Schiphol airport. The biometric access card allows members to pass some control points after verification of the identity of the holder of the card by the iris. This system is set up in cooperation with the border control authorities (public-private cooperation).

2.2.5 Standardization Efforts in the Field of Biometrics

172. Many efforts are being undertaken in the field of the standardization of biometric data processing on the national and international level.[256]

173. First of all, national governmental bodies look into aspects of the processing of biometric data which need to be coordinated and standardized. The German Institute for Standardization (‘*Deutches Institut für Normung*’) (DIN), the Biometric Working

[252] P. De Hert and A. Sprokkereef, ‘Germany’ in E. Kindt and L. Müller (eds.), D13.4. The privacy legal framework for biometrics, Frankfurt, FIDIS, May 2009, p. 70 (‘De Hert and Sprokkereef, Germany, in Kindt and Müller, Privacy legal framework for biometrics, Fidis, 13.4, 2009’).

[253] For examples, see Part III, Chap. 7, §§ 163–166, in particular at the footnotes 398 and 399.

[254] See, e.g., in France. Specific regulation was adopted to facilitate the authorization of such systems. See Part II.

[255] See, e.g., in the United States, the requirement for loan originators to submit fingerprints allowing (implicitly) the creation of a national fingerprint registry for everyone involved in the mortgage business, allowing background checks (Housing and Economic Recovery Act of 2008, H.R. 3221, Section 1505).

[256] While standardization relates to many aspects, they relate mainly to biometric data interchange formats (e.g., for fingerprint images and minutiae sets, iris images, etc.), interoperability and data interchange. Beyond data exchange, the standardization of harmonized performance testing methods and reporting standards is essential in order to achieve fair and reproducible benchmarking.

Group (BWG)[257] in the United Kingdom, and the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI)[258] and the InterNational Committee for Information Technology (INCITS) in the United States are among the bodies which are most active in this field. They also often participate in the drafting of international standards.

174. International standards are discussed and approved in international organizations, such as the European Committee for Standardization (CEN)[259] in collaboration with the Information Society Standardization System (ISSS), the International Civil Aviation Organization (ICAO), the International Labor Organization (ILO) (two UN related organizations) and the International Standardization Organization (ISO). The ISO standards are the result of collaborative efforts whereby worldwide national needs and requirements – formulated by governmental (standardization) bodies, professional groups and experts – are taken into account. For this reason, the process of getting a final ISO standard approved takes quite some time.[260] The ISO standards, although not binding, are important because once approved, they allow companies to make assertions and to have their claims certified by outside auditors. Standards are also increasingly referred to in legislation. In case the wording of such legislation imposes an obligation to follow a particular standard, such standard will be binding.[261] After some fixed period, final standards are again under review. The work of ISO, based in Geneva, Switzerland, in cooperation with the International Electro-technical Commission (IEC) in the field of biometric systems is important and is therefore briefly described hereunder.

---

[257] See www.cesg.gov.uk. The UK BWG supports the UK government in its current and future use of biometric data for personal identification and authentication. BWG is managed by CESG. CESG is the UK Government's National Technical Authority for Information Assurance.

[258] See www.ansi.org

[259] See www.cenorm.be. CEN is the European Committee for Standardization, which draws up voluntary technical specifications to help achieve the Single Market in Europe. The CEN/ISSS Biometrics Focus Group held its first meeting in Brussels, Belgium in June, 2004 and will address biometric interoperability for travel by European citizens in- and outside the EU and EFTA, travel within the EU by non-EU residents, cross-jurisdictional e-government services, and access control by multinational organizations.

[260] Typically, an expert group develops an initial draft standard, which is sent out for review and comments by a specific date. The expert group then reviews the comments and sends out a revised draft for another round of reviews and suggested changes within a specific time period. This may be repeated various times, after which – usually years – a standard becomes final and is published. See also *above* about the adoption of an ISO standard on biometric vocabulary.

[261] E.g., the Regulation No 2252/2004 (ePassport Regulation) refers in its Annex to ICAO Document 9303 (see also *above* § 162 and footnote 233). Although these guidelines of ICAO are technically speaking not a ratified or approved standard, they are sometimes also referred to as (*de facto*) standards. If legislation incorporates such guidelines or references to 'standards' in legal acts and imposes them, they become binding. For additional technical specifications for ePassports, in particular relating to the storage and the protection of fingerprint, see also Commission Decision of 28 June 2006 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States [C(2006)2909 final- Not published in the Official Journal].

175. Subcommittee 37 ('SC 37') of the Joint Technical Committee 1 ('JTC 1')[262] of ISO/IEC focuses on the standardization of biometrics. SC 37 was set up in December 2002 and consists of six Working groups.[263] Working Group 1 worked on the ISO Vocabulary for Biometrics.[264] Group 2 works on Biometric Technical Interfaces. The BioAPI is one of the standards on which that group has worked. Group 3 standardizes the Biometric Data Interchange Formats. This group has also been very active. It aims at standardizing the content, meaning, and representation of biometric data formats which are specific for a particular biometric technology. The standards for the biometric data interchange formats for fingerprint image (ISO/IEC IS 19794-4), face image (ISO/IEC IS 19794-5) and iris image (ISO/IEC IS 19794-6) issued in 2005 and some already revised are examples of well known standards of this group.[265] Group 4 works on a Biometric Functional Architecture and Related Profiles. Group 5 concentrates on Biometric Testing and Reporting and Group 6 on the Cross-Jurisdictional and Societal Aspects.[266]

The work of Subcommittee 37 is also relevant for and related with other standardization work within ISO, such as the work of the Subcommittees 17 (Cards and Personal Identification) and 27 (Security Techniques) of the Joint Technical committee 1 of ISO/IEC. Working Group 5 of Subcommittee 27 has been involved in the standardization of so-called 'protected templates' for biometric data processing which we consider important.[267]

The standards which are on the international level currently being developed for the processing of biometric data are hence numerous.[268] In addition, a lot of future work is planned and still to be done.[269]

176. The standardization of technical aspects of the processing of biometric information has without doubt a positive effect on the interoperability of biometric data

[262] JTC 1 of ISO/IEC is responsible for the international standardization in the field of Information Technology.

[263] SC 37 was set up following a US proposal in 2002 for a specialized subcommittee dedicated to biometric standards. Standardization activities related to cards and personal identification are excluded from SC 37 (these activities are taken up by SC 17) as well as biometric protection techniques, biometric security testing, evaluations and evaluation methodologies (these are treated in SC 27).

[264] See also *above*, §§ 96–97.

[265] ISO 19794 also includes parts for e.g., signature/sign behavioural data, human vascular biometric (vein) images, hand geometry, voice data and DNA data, some already adopted and others under development. See also for an overview, including related files of the meetings of SC 37 Group 3, Ch. Bush, *Standards*, available at http://www.christoph-busch.de/standards-sc37wg3.html

[266] See also *below* in Part III, Chap. 8, § 200.

[267] See *below*, Part III, Chap. 8, § 315 *et seq*.

[268] So far, the Subcommittee 37 adopted and published under its responsibility 80 ISO standards (including revisions). For an overview of the international standards published and under development, see ISO/IEC JTC1 SC37, Biometrics, available at http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770

[269] For future work of SC 37, see ISO/IEC JTC1 SC37, Biometrics, available at http://www.iso.org/iso/jtc1_sc37_home

processing and data interchange. Industry and interested parties in the field of biometrics will therefore be aware of the (draft) standardization documents issued by these international and national standardization organizations in their interest. Whether such interoperability is always desirable from the point of view of privacy and data protection, however, will be discussed *below*.

2.3 Preliminary Conclusions

177. Biometric characteristics have *since long* been used by persons to recognize known or unknown individuals and to identify them. Biometric systems differ from the previous use of unique or distinctive human characteristics in that now *systems store* the *unique* and *persistent* characteristics for *automated* comparisons. Biometric systems, being developed since a few decades, are however *very complex* systems and their functioning are mostly only understood by experts.

178. In the meantime, biometric systems have been introduced in (very) *large-scale* implementations, meeting a societal *need for more security* and *efficient cooperation*. These systems deployed by the governments initially focused on third country nationals (foreigners, such as asylum or visum applicants) (for example, Eurodac and VIS) and criminals (SIS and SIS II). Biometric systems, however are gradually expanding to Union and Member State nationals (for example, the introduction in 2004 of the biometric ePassport in the Union Member States) without profound public debate. Furthermore, the purposes of these systems are often broadly formulated, or, if the initial purposes were limited, the purposes and access to the databases were in several cases expanded (e.g., VIS). In addition, biometric systems are coming in every one's day to day life in the private sector, sometimes at a young age, for example, for access control in schools.

179. In order to facilitate the debate about the use of biometric systems, including an analysis of its legal aspects, a sound understanding of the functioning of biometric systems and of their main features, including of some more technical aspects, is required but is often lacking. We have therefore described in this first Chapter how biometric systems are based on measurements and statistical methods, with *inherent errors*, which have to be taken into account. Because of the intra-class and interclass variability of the characteristics measured, the comparison is and will *never be 100 %*, even though the technology is continuously being further developed, and biometric systems remain 'inherently fallable'.[270] One shall therefore understand that biometric systems are because of the error rates not apt to offer 100 % security or convenience and that the efficiency for this reason is sometimes questionable.

Many elements influence the process, some of which may be determined by the controller(s) of the system (e.g., choice of characteristic, use of a database or not,

[270] NRC, Biometric Recognition, 2010, p. 1: 'Human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated'.

decision about the threshold and the acceptable false acceptances, qualified staff, control of the quality of the data), but also by developers, while others may be out of control (e.g., failures to enroll, illumination conditions). The *accuracy* which can be reached with biometric systems therefore remain conditional or uncertain. This may affect the finality and the proportionality of the processing of the biometric data, as well as require additional measures, as we will argue in Part II and III. Because of test and evaluation issues, it is also very difficult to provide uniform accuracy rates of a system in an operational environment. As if this would not suffice, there are other risks and insecurities which are linked with the use of biometric systems and which we explain in Part II, Chap. 4.

We also stressed in particular that biometric systems can be used in substantially different ways, in particular for either *searching* the identity and *identifying* a person, or for *verifying* whether a claim (e.g., relating to a right or an identity) is true. We touched upon the issue that the identification functionality poses specific (technical) challenges to the systems. Examples are VIS and SIS II which envisage to use the *identification* functionality, while this is, for example for SIS II, *not yet operational*. Furthermore, one needs to understand that the identification offered by the system will only be secure and reliable if previous to the enrolment an adequate control of the link between the person and the claimed identity is made.

Overall, it should be clear that the results which a biometric system may offer, is for each use and application different and *is not* "*plug and play*".[271]

180. Chapter 2 has given a brief and general introduction in these highly specialized technical aspects of biometric systems and described some current applications, including some standardization activities.

In Chap. 3, we attempt to qualify biometric data from a legal point of view and propose a working definition for biometric data. We also compare biometric data with other categories of personal data which show similarities with biometric data, in particular DNA information, and take a look at the regulations applicable to these data. We will also explore whether and how the fundamental rights of data protection and privacy are relevant and apply to the biometric data processing.

[271] J. Wayman, *Biometrics & how they work*, slide 91, San Jose State University, 2002, available at http://www.cfp2002.org/proceedings/proceedings/jlwcfp2002.pdf

http://www.springer.com/978-94-007-7521-3

Privacy and Data Protection Issues of Biometric Applications
A Comparative Legal Analysis
Kindt, E.J.
2013, XXI, 975 p. 11 illus., Hardcover
ISBN: 978-94-007-7521-3