The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective

Els J. Kindt

The Use of Privacy Enhancing Technologies for Biometric Systems Analysed from a Legal Perspective

Els J. Kindt

Abstract. The deployment of biometric systems could have serious life long implications for the privacy and data protection rights of individuals. The use of appropriate biometric technologies permitting the creation of multiple trusted revocable protected biometric identities may present a response to this challenge. The paper presents a review from a legal perspective of these privacy enhancing technologies which are being developed in the 7th framework EU project TURBINE. It is argued that if privacy considerations are taken into account in the design and technology of biometric systems, this will have a positive influence on the review of the proportionality of the use of biometric systems.

Introduction

Biometric technologies are increasingly applied in identity management systems as a more secure solution for identity verification, for example for access control in a company or for online applications. However, because of the unique link with a person, the use of biometric characteristics has also caused many serious concerns. These include the potential use of the biometric data for linking information about persons within or across various information sources and the undesired re-use of biometric information for purposes which were not initially envisaged at the collection of the data, for example for profiling or surveillance purposes. Moreover, biometric data may reveal sensitive information, and last but not least, the biometric characteristics used remain in principle persistent over years and cannot be re-issued if compromised. In case of abuse of biometric data (e.g., for identity theft purposes), this will render the life of the victim quite burdensome in proving that he or she has not committed the offences or crimes whereby his or her 'stolen' biometric data were used, if not impossible.

Many of these privacy and data protection issues have been identified and discussed by national Data Protection Authorities and in the Article 29 Data Protection Working Party document on biometrics of August 2003.[1] The

[1] Article 29 Data Protection Working Party, *Working document on biometrics, WP 80*, 1 August 2003, 12 p.

Working Party in this document called upon the industry to develop biometric systems that are privacy and data protection compliant.

In this paper, it will be discussed whether and under which conditions the local storage of biometric characteristics on an object under the control of the data subject is effective in enhancing the privacy protection. In addition, other features and aspects of biometric identity management systems are particularly relevant for making systems data protection compliant 'by design'. Some of these features will be further described. This will primarily be done by means of discussing the research and the developments in the 7th framework EU project TURBINE, which focuses on the development of trusted revocable protected biometric identities.[2] It is argued that where the privacy is included in the design, this will influence the review of the risks of the use of biometric characteristics as compared with the benefits, also referred to as the proportionality issue. Finally, the features discussed could lead to the formulation of best practices in the use of biometric characteristics for the enhancement of identity management systems and certification.

1. Biometric data under the control of the data subject

The concept of control by the data subject has been put forward at regular times as an important element of privacy. Alan F. Westin defined in 1967 privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others.[3] Westin therefore sees privacy as a form of autonomy, in particular, the ability to control the flow of information about oneself. Arthur R. Miller wrote in 1971 that 'the basic attribute of an effective right to privacy [is] the individual's ability to control the flow of information concerning or describing him'.[4]

The Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Data Protection Directive 95/46/EC, however, gave a far more limited role to control over personal data

---

[2] TrUsted Revocable Biometric IdeNtitiEs project (TURBINE), EU project no. 216339 (2008-2011), www.turbine-project.eu .See also J. Breebaart, C. Bush, J. Grave and E. Kindt, 'A reference architecture for biometric template protection based on pseudo identities', in A. Brömme (ed.), *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Bonn, Gesellschaft für Informatik, 2008, pp. 25-37.

[3] A. Westin, *Privacy and Freedom*, New York, Atheneum, 1967.

[4] A. Miller published in 1971 in the United States the book 'The Assault on Privacy', in which he examined the effect of the technological revolution (of that time) on individual privacy. He made various proposals to reconcile technology with society values, which aroused discussion and controversy. See A. Miller, *The Assault on Privacy: Computers, Data Bases and Dossiers,* Ann Arbor, University of Michigan press, 1971.

or to applications controlled by the users. These legal instruments attempted to reconcile the demand for a free flow of personal data with the right to privacy of individuals. Because of the type of processing of personal data, at the time of enactment of the Convention and the Directive mainly by mainframe computers, the articles did not provide for an express right for the data subject to control his or her personal data, but rather for information rights (transparency) and access and correction rights. Some countries, however, in particular Germany, provide for a constitutional right to informational self-determination. The German Federal Constitutional Court has, based on the 'general right of personality' of the Constitution[5], recognized various expressions of this right, including the right to respect for privacy in 1970, and the right of informational self-determination in 1983.[6] This right to informational self-determination is important for the data protection legislation in Germany. Partly due to the changes in the use of computers, applications and the worldwide network infrastructure, the concept of individual control gains more and more attention and support, also in other countries of the European Union. At the same time, it should be admitted that control over information, including over personal data, remains on the conceptual level problematic.[7]

Privacy thought of as *the right to decide over and to control personal information* is of particular importance for biometrics. The Data Protection Directive 95/46/EC, however, does not contain any specific provisions supporting individual control. It lacks, for instance specific requirements relating to the place of storage of personal data, which is a central issue regarding biometric data. In case of central storage of biometric characteristics, use of the characteristics for identification without knowledge of the data subject and re-use for other purposes are amongst the fears and

---

[5] The German Federal Constitution of 23 May 1949 contains two articles which are important to understand the 'general right of personality', specific for Germany : Article 1 (1) which establishes the fundamental right of protection of human dignity and Article 2 (1) which states the fundamental right to develop freely one's personality.

[6] BVerfG, 15 December 1983, *BVerfGE* 65, 1. This right to informational self-determination heavily determines and weights upon the interpretation of the data protection legislation. See also G . Hornung and Ch. Schnabel, 'Data protection in Germany I : The population census decision and the right to informational self-determination', *Computer Law & Security Review*, 2009, pp. 84-88.

[7] Many legal scholars reject the idea of ownership rights in information and/or data. Some maintain that only intellectual property rights could govern any rights in relation to information. Questions remain as to the enforceability of a right to control and protect information, not only against contracting parties but also against third parties. Ownership over data in databases however may become more accepted. See also E. Kindt, 'Ownership of Information and Database Protection', in J. Dumortier, F. Robben and M. Taeymands (eds.), *A Decade of Research @ the Crossroads of Law and ICT*, Gent, Larcier, 2001, pp. 145 – 160.

risks which are put forward.[8] Local storage on an object under the control of the individual has been therefore suggested[9] and may be one of the most important methods to protect biometric data because it allows the data subject to control the use of the biometric characteristics and serve as protection against attacks of central databases.

Individual control over biometric data has almost become a requirement for privacy compliance by some national Data Protection Authorities (DPAs).

In 2000, The French DPA, the CNIL, rendered several opinions with regard to the use of fingerprints in the private sector and which were (to be) centrally stored for a variety of purposes. The CNIL underlined that that fingerprints were not only mainly used by the police in the past, but that a database with fingerprints is likely to be used by the police in the future as well, and is to become 'a new instrument of the police', irrespective of the original purposes of the processing.[10] The CNIL has thereupon developed a position on the use of biometric identifiers (in particular fingerprints) which shall in principle not be stored centrally for the reasons set out above, but which shall be stored locally, on an object in the possession and/or under the control of the data subject (for example, on a smart card or a token). Other DPAs are following this position and have also given advice and guidelines not to store biometric data centrally.[11] The central storage has also been considered a major element for the decision on the infringement of the fundamental right to respect for privacy in case law of the European Court of Human Rights.[12] At this point, what is clear is that besides centralized or federated identity management systems, user-centric identity management, where the user can make choices, comes into view. New models 'involve (…) the users in the management of

---

[8] Biometric data is increasingly stored in central databases, not only in the private sector, but also for government use. In the Netherlands, for example, the Passport Act, which was modified further to Regulation 2252/2004, now provides for the central storage of fingerprints upon application for a travel document (see Art. 4a paragraph 2b of the Act of 26 September 1991 containing the rules for the issuance of travel documents, as modified by the Act of 11 June 2009 modifying the Passport Act relating to the modification of the travel document administration, the latter published in *Stb.* 2009, 252, also available at https://zoek.officielebekend makingen.nl/stb-2009-252.html).

[9] See for example, the Dutch DPA in its report At Face value : R. Hes, T. Hooghiemstra and J. Borking, *At Face Value. On Biometrical Identification and Privacy,* Achtergrond Studies en Verkenningen 15, The Hague, Registratiekamer, September 1999, p. 52 ('At Face Value Report'). Shortly before, the Dutch DPA had stressed the use of privacy-enhancing technologies in its other report by R. Hes and J. Borking e.a. (eds.), *Privacy-enhancing technologies : the path to anonymity,* Den Haag, Registratiekamer, 1999.

[10] CNIL, *21e rapport d'activité 2000*, Paris, CNIL, p.108.

[11] For example, the DPAs of Greece and Belgium.

[12] See ECHR, *S. and Marper v. U.K.,* nos. 30562/04 and 30566/04, 4 December 2008.

their personal information and how that information is used, rather than to presume that an enterprise or commercial entity holds *all* the data'.[13]

The local storage of biometric characteristics, in particular fingerprint, is one of the aspects researched in the 7th framework programme research project TURBINE. It proposes a user-centric IdM system model, which allows the data subject to manage its identities and the personal information released. TURBINE's research concentrates on the transformation of fingerprints of an individual into several unlinkable 'pseudo-identities' for different applications based on the same fingerprint. Various architectures are presented and reviewed in the project. After elaborating the various options, the local storage of the biometric characteristics such as on a token under the control of the data subject or on secured hardware with a 'match-on-card' functionality, is further researched and tested because of its privacy-enhancing potential.

Control by the data subject, however, *is not limited* to *physical control* over the object on which the biometric characteristics are stored. Control also requires that there are tools provided for the data subject to obtain information about the process in which his or her characteristics are used for identity verification or authorization (output), and to provide instructions (input).[14] Such input could, in case the application provides for multiple identities, for example, be the selection of one of the identities.[15] TURBINE, for example, for its demonstrators has defined a user interface, which is a component that can be integrated and which will enable the data subject to provide/receive such in- and output. Any data transfer from or to the on-token data storage may be controlled (by means of the 'pseudo identity selector' implemented on the token[16]) and needs to be approved by the user through this interface. The interface would also provide for an opportunity to implement a multi-layered information notice to the data subject, enriched with additional information that is required to make the biometric system transparent for the person concerned. A multi-layered information notice is referred to by the Article 29 Working Party in an Opinion on harmonized information provisions in

---

13 Prime, *Prime White paper*, 2008, v.3.0, p. 2, available at https://www.prime-project.eu/prime_products/white_paper/PRIME-Whitepaper-V3.pdf ('Prime White paper ') The text was cited from the *Liberty Alliance Project Whitepaper : Personal Identity*, 23 March 2006, available at http://www.projectliberty.org/liberty/content/view/full/340/(offset)/30 .

14 Compare with the Prime-console, intended to allow the data subjects to manage their personal data (see Prime White paper, pp. 8-9).

15 See also the so-called 'Identity protector (IP)' mentioned by the Dutch DPA which shall be seen 'as a part of the system that controls the exchange of the user's identity within the information system'. See At Face Value report, p. 62.

16 The token does not merely provide data storage, but also implements intelligent access control for the stored data.

2004.[17] It would essentially allow controllers to employ a simplified short notice in their user interface, as long as the latter is integrated in a multi-layered information structure, where more detailed information is available, and the total sum of the layers meets national requirements.[18] The additional information could include information about the biometric process, such as confirmation of the use of the verification functionality, the place of storage, error rates, the deletion of copies of biometric characteristics, security measures, and about alternative means in case of failure of the system.

The improved control by the data subject in the TURBINE project, however, would not imply that the data subject can access the protected biometric identity. There is only a 'partial access control' by the data subject: the data subject *holds* the token, *induces* the verification based on the biometric characteristic by presenting the life sample and also because the data subject may *select* an identity.[19]

Various architectures and technical solutions with a user-centric approach other than TURBINE have been developed, tested and used as well.[20]

Other means for control over personal data by the data subject have been suggested. For example, the central storage of biometric data, which can only be accessed after input by the data subject of username with PIN.[21]

In any case, the conditions of a local biometric storage under which the control of the data subject may be effective remain important and need to be

---

[17] The Article 29 Working Party, Opinion on More Harmonised Information Provisions, 25 November 2004, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

[18] More specifically, the Article 29 Working Party envisages that there could be up to three layers of information: (i) the *short notice*, which provides the essential information (and, in view of the circumstances, any additional information necessary to ensure fair processing); (ii) the *condensed notice*, which includes all relevant information required under the Data Protection Directive; and (iii) the *full notice*, which includes all national legal requirements and specificities.

[19] Some also refer to a so-called 'divided control model' when the biometric data and the usage of the device is controlled by the data subject, while the processing itself is controlled by an organisation acting as controller. See E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, Fidis, 2007, 130 p., available at www.fidis.net

[20] For example, Priv-ID, see http://www.priv-id.com/; see also the proof of concept of 'encapsulated biometrics' of the AXS Internet Passport, described in L. Müller and E. Kindt (eds.), D3.14 Model implementation for a user controlled biometric authentication, Frankfurt, Fidis, August 2009, 57 p., available at www.fidis.net

[21] See R. Van Kralingen, C.Prins and J. Grijpink, 'Het lichaam als sleutel', *National Programma Informatietechnologie en Recht*, 8, Alphen aan den Rijn/Diegem, Samsom BedrijfsInformatie Bv, 1997, p. 20. See also e.g., Biermann, H., Bromba, M., Busch, C., Hornung, G. ,Meints, M. and Quiring-Kock, G. (eds.) *White Paper zum Datenschutz in der Biometrie,* 2008, available at http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf.

reviewed and evaluated on a case by case basis. These conditions are not always clearly specified by the various national Data Protection Authorities[22] and advocates of privacy enhanced biometrics systems who stress the importance of the concept of control by the data subject. Some opinions of the DPAs on same or similar issues are even divergent. At least, one will note that some opinions contain far more detailed requirements in setting out the conditions for the processing of biometric characteristics than others.

2. Other elements by design which enhance privacy

Other features, such as the transformation of the data[23], in addition to control by the data subject, however, are also important and needed to protect one's privacy. These elements are in most cases not specified as such in data protection legislation. In order to be effective, the features shall be embedded from the start in the architecture of the biometric system. It is interesting to note that discussions about privacy in the architecture and design of a system in fact refer to a more technical understanding of privacy, such as preventing unintended leakage of information. Particular privacy threats in systems which are mentioned include surveillance (i.e., the monitoring of electronic communications and transactions), the aggregation of information (i.e., the linking of information as related to each other or to a particular subject) and use for profiling, and identification (i.e., connecting information to a person). Privacy protecting concepts in an architecture from a more technical point of view and which are crucial for privacy thus include unlinkability, unobservability, anonymity and pseudonymity.[24] Below, we discuss some of the privacy enhancing technologies developed in TURBINE that supplement control by the data subject.

Issuance of multiple identities and limitation of the ability to link - In theory, a unique human characteristic will give a very similar digital presentation each time the characteristic is used (provided some conditions are fulfilled, such as, for example, the use of the same algorithms and methods). As a result, information from databases which use the same characteristic (and provided the same technologies are used) can be related to one and the same

[22] However, compare with the N°AU-019 of the French DPA, the CNIL, which, in addition to the general legal security requirement, contains supplementary and detailed requirements relating to security for the Unique Authorization (UA) for vein of fingers analysis (Article 6).

[23] Such transformation would not only protect the data but could for example also permit the issuance of multiple revocable identities, as will be discussed below.

[24] See A. Pfitzmann and M. Hansen, Anonymity, Unlinkability, Undetectability, Unobser-vability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version v.0.31 Febr. 15, 2008), available at http://dud.inf.tudresden. de/literatur/Anon_ Terminology_v0.31.pdf

person and can be combined.[25] A privacy-enhancing requirement for biometric systems is therefore the transformation and manipulation of the biometric data such that different identities can be issued.[26] The possibility to issue multiple identities is important because it is essential for protecting the privacy of the individuals involved upon the use of their unique human characteristics. This, far from being a trivial requirement is a main topic of research in the Turbine project.

In addition, further manipulation of biometric data is needed to limit the ability to link identities and the related personal data from different databases. Turbine develops technology and methods for the limitation of the use of a protected biometric identity *in a specific situation or for a specific service* whilst ensuring that these different identities (and the personal data linked with a specific biometric identity) cannot be linked to each other (excluding the risk of cross-linking). This is done by combining the protected binary identity derived from the captured biometric sample with a service identifier which limits the use of the biometric identity to a specific service context. In this way, and with help of cryptographic techniques, the pseudo identity based on the biometric characteristics is meaningless outside the service context.

Deletion of image and unprotected template - A further privacy enhancement can be achieved by not storing the original image of the biometric characteristic or any intermediate data between the extraction steps and the protected template. The source data and the unprotected template should *always be deleted* after the extraction process for enrolment or comparison. Such deletion does not only apply to the local device (such as e.g., the biometric scanner), but also to all other components of the biometric system. This could also be confirmed to the data subject during the process. Only under this condition can the possible misuse of the image or template, such as the use as a unique identifier for combining all information linked with a specific biometric identity or the use of possible sensitive information contained in the image or template be prevented.

Revocation and re-issuance - Another important feature is the possibility to re-issue a protected biometric identity, in case a previously issued protected biometric identity would be compromised or lost (possibility to revoke). The fact that the biometric characteristics of a person are unique and persistent and can in principle not be changed in case of abuse has always been one major concern for biometric systems. This concern can be overcome if an identity

---

25 This issue is also referred to as the use of biometric data as unique identifiers.

26 Multiple identities combined with accountability is also proposed as a requirement in the Prime White paper for identity management systems in general. See Prime White paper, p. 11. Accountability refers to the possibility to make the link back to the individual if needed.

provider could issue more than one biometric identity which can be revoked. This has been researched for some years [27] and several methods for such 'revocable biometrics' have been proposed now. The possibility to revoke a biometric identity is equally tested and demonstrated in TURBINE. For this purpose, the template protection process includes means for the generation of multiple independent protected biometric identities from the same biometric characteristics. The process of generating multiple independent protected identities from the same biometric characteristics is referred to as 'diversification'. The technology developed in TURBINE provides the individual with the option to revoke an identity for a given application in case of need. Various privacy advocates and some DPAs have pointed to this important privacy-enhancing aspect for biometric systems.[28]

Protected templates – The biometric identities which satisfy the aforementioned requirements, during storage, transmission and comparison operations, are in TURBINE referred to as 'protected biometric templates' or 'protected templates'.[29] From such templates, it should also *be impossible to reverse engineer (i.e., retrieve or recode)* the original biometric image, features or template, or any derivatives that reveal 'sensitive' information from the biometric sample (such as health related data). A further feature of protected templates is that they allow for the use of pseudonymous identities without revealing the 'real' (in particular, 'civil') identity of the data subject. For this to work on a larger scale, some forms of standardization are required. Efforts to achieve such standardization of some aspects of protected templates are under way.[30]

'Anonymous' access control mechanisms - While biometric characteristics facilitate in essence the identification of person or the verification of an identity or pseudonym, it is not always required that the biometric data are used in such a way. If there is no need for identification or verification of the identity or pseudonym, '*anonymous' access control mechanisms* deploying

---

27 See, for one of the first publications, N. Ratha, J. Connell, and R. Bolle, 'Enhancing security and privacy in biometrics-based authentication systems' IBM systems Journal, vol. 40, 2001, pp. 614-634.

28 See A. Cavoukian and A. Stoianov, Biometric encryption : a positive-sum technology that achieves strong authentication, security and privacy, Privacy Commissioner Ontario, 2007, available at www.ipc.on.ca

29 About the concept of protected templates, see also U. Korte, J. Merkle, M. Niesing, 'Datenschutzfreundliche Authentisierung mit Fingerabdrücken. Konzeption und Implementierung eines Template Protection Verfahrens – ein Erfahrungsbericht', Datenschutz und Datensicherheit 2009, pp. 289 – 294.

30 See J. Breebaart, B. Yang, I.Buhan-Dulman, Ch. Busch, 'Biometric Template Protection. The need for open standards' in Datenschutz und Datensicherheit 2009, pp. 299-304.

biometric characteristics stored on the token may be used to manage the authorization of a given person to an area or place.[31] A scheme based on group signatures and encryption allows access for a data subject without verification of the identity. The biometric data stored on the token or card and a local on-card or off-card matching of biometric data allow the cryptographic keys and computational mechanisms stored on the smartcard to be unlocked. The service provider can thus verify whether the anonymous user who accesses the service or place belongs to a group of authorized data subjects. The biometric characteristics are in this case hence not used for the authentication, i.e., the verification of the correct user, but only for the authorization check. Some DPAs have pointed to the need to deploy such mechanisms in case there is no need to check or verify the identity of a person. The Belgian DPA, for example, stated that this way of access control is important in the evaluation of the proportionality of a system.[32] The scheme as developed in TURBINE, allows for de-anonymization in case of need (semi-anonymous access control).

Identity management organisation – The overall organisation of a privacy enhanced biometric identity management system is an important topic. First, the roles of the identity and service providers should be clearly defined. It shall also be specified for which components of the biometric system, data and data flows they bear responsibility. This responsibility shall relate in the first place to data protection and compliance in general, including data breach. The access control regarding agents and personnel of the identity provider and service provider to the information stored in the biometric system is therefore an important requirement. Moreover, identity and service providers shall also be responsible for the functioning of the specific components of the biometric system and possible failure. For this reason, they will have an interest to obtain representations and warranties from the manufacturers of the systems.

Another central issue is how the identity or the credentials of an individual shall be established prior to enrolment. The promised enhanced security of biometric systems is only guaranteed if clear agreements are made between the stake holders involved on how individuals need to prove their identity or the necessary credentials. This is especially important in case the biometric identity would be used for authenticating the civil identity.

---

31 Compare with the use of anonymous credentials, as set forth in Prime White paper, pp. 10-11.

32 Commission for the Protection of Privacy, Opinion upon own initiative concerning the processing of biometric data in the framework of the authentication of persons, Opinion N° 17/2008 of 9 April 2008, p. 19.

3. The proportionality issue

An important question regarding the legality of the use of biometric systems is whether such a system is proportionate to its purposes. The proportionality requirement refers to a general principle of law, which has its origin in mainly public law.[33] In general, the principle requires a fair balance and reasonable relationship between the means used and the objective(s) sought. To the extent that a chosen application would present privacy and data protection risks for the data subject, the proportionality test requires that the risks of the application do not outweigh the interests and benefits sought by the controller. The proportionality principle is reflected in various articles of the Directive 95/46/EC, including in the provision that states that personal data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed' (Article 6.1 (c)). If a biometric system allows the deletion of the original image and the unprotected templates and uses protected templates, from which it is in principle not possible to reverse engineer the original biometric image or template, and which do not permit the linkage of data from different databases but allow the issuance of multiple identities, such biometric system is using best efforts for meeting the aforementioned requirement that the system shall use data which are not excessive.

Article 7 of the Directive 95/46/EC contains as a ground for making the data processing legitimate that the processing is necessary for the legitimate interests pursued by the controller except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The risks of using unique identifying human characteristics in automated applications have been described at length in many reports.[34] These risks include the cross-linking of information, the re-use of information for other purposes than those initially envisaged, the use of sensitive information contained in biometric data and the impossibility to re-issue biometric characteristics. If the technological design and subsequent implementation is able to limit (or exclude) most or some of these risks associated with the use of biometric characteristics, the use of such biometric systems for particular objectives will be in a better balance with the aims that are sought. Limiting

---

[33] In public law, the proportionality principle lays some fundamental rules for justifying state interference with the fundamental rights and freedoms of individuals. On the proportionality of biometric systems, see also E. Kindt, 'Biometric applications and the data protection legislation', Datenschutz und Datensicherheit (DuD) 2007, pp. 166-170.

[34] See, for example, J. Goldstein, R. Angeletti, M. Holzbach, D. Konrad, M. Snijder, *Large-scale Biometrics Deployment in Europe : Identifying Challenges and Threats*, P. Rotter (ed.), JRC Scientific and Technical Reports, European Commission JRC – IPTS, Seville, 2008, 135 p ; see also E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, 130 p.

the risks by one or more 'privacy by design' elements which enhance the privacy of the data subject as described above, could therefore have a positive influence on the evaluation of the interests of the data subject who may have fewer objections against the use by the controller of biometric data for legitimate interests. Finally, the Directive 95/46/EC requires that the processing shall be lawful (Articles 5 and 6.1(a)). The latter implies that the system shall not only comply with the specific data protection requirements, but also that, in conformity with Article 8 of the European Convention on Human Rights and Article 7 and 8 of the Union Charter, it shall be reviewed whether the processing is interfering with the *fundamental rights* to respect for privacy and data protection. If interference remains, it shall be 'necessary in a democratic society'. [35] The necessity can only be proven if one can show that there is a 'pressing social need' to use a biometric system, that the system is 'relevant and sufficient' and that the processing of biometric data is proportional with the legitimate aim. Using privacy enhancing technologies will in our view reduce the interference with fundamental rights and improve the required proportional use. The DPAs who have reviewed biometric systems sometimes require that the security reasons for deploying a biometric system shall be of a more important general nature[36] than the security needs of the controller alone. On the other hand, DPAs have imposed no stringent requirements as to the need to show that a biometric system is relevant and sufficient. With regard to the proportionality review, 'privacy by design' is taken into account by various DPAs in so far that the DPAs have a clear preference that biometric data are not stored in a central data base, but on an object under the control of the data subject. However, many other technical specifications as to how such data which are locally stored may be used, are not provided by most DPAs. The local storage of biometric data on an object under the control of the data subject will in our opinion only be effective if other conditions are fulfilled. These conditions include that even if the biometric data are locally stored, biometric data shall not be copied during enrolment or later comparison in a central database. In addition, the use of protected templates which exclude the possibility of linking information and which permit the issuance of several biometric identities based on the same characteristics should also be considered. Clear information and transparency on how the biometric data is used and processed is also essential, while in some cases more control over the biometric identities should be given to the data subject. Choosing a biometric system whereby the privacy is included in the design combining the discussed privacy-enhancing technologies and

---

[35] This comes in addition to the need of some basis in domestic law (which is accessible and foreseeable) and a legitimate aim. These requirements will not be further analysed herein.

[36] For example, the need to secure access to a nuclear power plant is of a more general (public) interest than the interest of the controller alone.

features will have a positive effect on the requirement of the proportional use of biometric applications.

Conclusion : Towards best practices

The discussion above should further induce the discussion and the formulation of best practices for the privacy friendly processing of biometric data. Best practices are a way of self-regulation which is often promoted by stakeholders of a particular sector. In the past, there have been initiatives promulgating best practices for biometrics, such as the Privacy Best Practices in Deployment of Biometric Systems of the BioVision project.[37] These proposed best practices however need to be reviewed in the light of the advancements of the biometric techniques and should aim in the first place to counter or limit as much as possible the most serious risks involved in the processing of biometric data and which relate to the special nature of biometric data.

The best practices in relation to the development and deployment of a biometric system will in general always depend upon compliance with data protection provisions, including the need for legitimate purposes and interests of the controller to use such system. The processing of biometric data, however, requires further 'best practices'. They would include, from a more general perspective, the deployment of irreversible and unlinkable templates which allow the deletion of the biometric images and unprotected templates. In addition, multiple biometric identities which can be revoked in case of misuse or any other need should be deployed. Moreover, only the verification function of a biometric should be used and the biometric data should be stored in a decentralized way. Additional specific security measures, including deploying cryptographic methods, limited access to any biometric data and a clear deletion policy, should be described as well. With regard to the enhanced rights for the data subjects, data subjects should be entitled to pseudonymity[38] and 'anonymity'[39] upon the use of a biometric system as much as possible. From an organizational and legal point of view, there should be a strict limitation of the use of a biometric system to either a private sector use or a governmental use. Furthermore, the functioning of the biometric system should be transparent for the data subject. This would imply

---

[37] BioVision, *Privacy Best Practices in Deployment of Biometric Systems,* August 2003, 49 p.

[38] Pseudonymity would in this context mean the right for the data subject to choose a pseudonym biometric identifier which does not allow to identify the data subject directly.

[39] 'Anonymity' in this context would be 'anonymous' comparison whereby the identity of the data subject is not stored or revealed.

extending the information provision to the data subjects and increasing control rights. They should also receive additional information about the most essential properties of the comparison system and the alternative procedures in case of failure of the system.
Because biometric products and systems are difficult to evaluate as to their technical operation and effects by non-technical persons, such biometric products and systems may need to be reviewed by experts, both IT-experts but also legal experts. This would lead to the certification of the biometric products and systems relating to its privacy-enhancing characteristics and privacy-compliance in a certification program which also take the privacy regulations in a consistent way into account. [40]
Such best practices in combination with certification could render the application of the (sometimes complex) legal regulation more clear. The European Privacy and Data Protection Authorities have called for legislation that will encourage the development and adoption of best practices, including privacy by design.[41] These efforts could finally result in a responsible use of one's biometric data in systems throughout one's life.

Acknowledgements : This paper is based on research in the 7th framework EU project TURBINE supported and funded by the EU Commission and is made possible because of the contributions by all partners to the project (see http://www.turbine-project.eu). The author thanks Koen Simoens of K.U.Leuven, COSIC, Belgium for the review of this paper and his valuable comments. The paper is representing only the author's view and is not binding on TURBINE partners or the European Commission.

[40] An example of a European wide certification scheme which provides a privacy trust mark for end-users (but which is not typical for biometric systems) is EuroPriSe. See EuroPriSe, EuroPriSe Criteria, v.1.0, available at https://www.europeanprivacyseal.eu/criteria/ EuroPriSe%20Criteria%20Catalogue%20 public%20version%201.0.pdf

[41] European Privacy and Data Protection Commissioners, Declaration on leadership and the future of data protection in Europe, Edinburgh, 23-24 April 2009, 1 p.