Misunderstandings in Misunderstandings on Biometrics

A Position Paper by the European Association for Biometrics (EAB)

Christoph Busch[1 2], Adam Czajka[3], Farzin Deravi[4], Pawel Drozdowski [1], Marta Gomez-Barrero[5], Georg Hasse[6], Olaf Henniger[7], Els Kindt[8], Jascha Kolberg[1], Alexander Nouak[7 9], Kiran Raja[2], Raghavendra Ramachandra[2], Christian Rathgeb[1 6], Jean Salomon[9], Raymond Veldhuis[10]

Abstract: The intention of this paper is to provide input and to comment on the joint EDPS-aepd publication "14 Misunderstandings with regard to Biometric Identification and Authentication" that was published in June 2020. It indicates what the members of the European Association for Biometrics (EAB) identified as missing information in the aforementioned publication. Our suggestion is to revise and augment the EDPS-aepd-publication, such that it includes a full picture of the current state of the art in biometrics and the availability of standards and privacy enhancing techniques.

Keywords: biometrics, face recognition; vulnerability analysis; border control

Introduction

Recently, the European Data Protection Supervisor (EDPS) together with the Spanish Agencia Española de Protección de Datos (aepd) has published a white paper entitled "14 Misunderstandings with regard to Biometric Identification and Authentication"[11]. The paper looks at biometric identification and verification[12],[13] and specifically focuses on fingerprint and face recognition. We assume that those 14 misunderstandings are myths that are spread through the people and that these statements come from the street.

Interested circles have studied the vulnerabilities of biometric technologies addressed in the White Paper and possible countermeasures for a long time. We definitely agree that biometric technologies are no universal miracle cure, but require the careful implementation of countermeasures against the threats they face, given the sensitiveness of biometric data.

The European Association for Biometrics (EAB) gathers multiple stakeholders interested and active in the domain of digital ID and biometrics in Europe. We are a non-profit, nonpartisan association. The EAB's mission is to tackle the complex challenges facing identification systems in Europe, in fields ranging from migration to privacy rights. Our role is to promote the responsible use and adoption of modern digital identity systems that organize, facilitate and/or enhance people's lives and drive economic growth. Through a series of EAB initiatives, we support all sections of the ID community across Europe, including governments, NGOs, industry, associations and special interest groups, and academia. Our initiatives are designed to foster networking and debate, either at EAB hosted events across Europe or run virtually, or in providing impartial advice and support to individual members. We ultimately serve the citizens of Europe in the advancement of modern digital biometric identity systems that are fair, accessible, secure and private.

Guaranteeing the privacy of individuals and the protection of biometric data through privacy enhancing technology (PET) is a driving motivation for many of EAB's activities, including workshops[14] and online meetings[15]. EAB hence reviewed the fore-mentioned publication and discussed with its members all the 14 topics addressed therein. We feel that the referenced literature is incomplete and therefore respond, with the intention to contribute to and to complement the said publication.

1. "Biometric information is stored in an algorithm"

It is true that certain biometric identification systems are trained on biometric samples obtained from the individuals to be recognised by the system. In these systems personal data may leak into the models, However, these systems

[1] Hochschule Darmstadt, Germany
[2] Norwegian University of Science and Technology, Norway
[3] University of Notre Dame, USA
[4] University of Kent, U.K.
[5] Hochschule Ansbach, Germany
[6] Secunet, Germany
[7] Fraunhofer IGD, Germany
[8] KU Leuven, Belgium
[9] European Association for Biometrics
[10] University of Twente, The Netherlands

[11] https://edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf

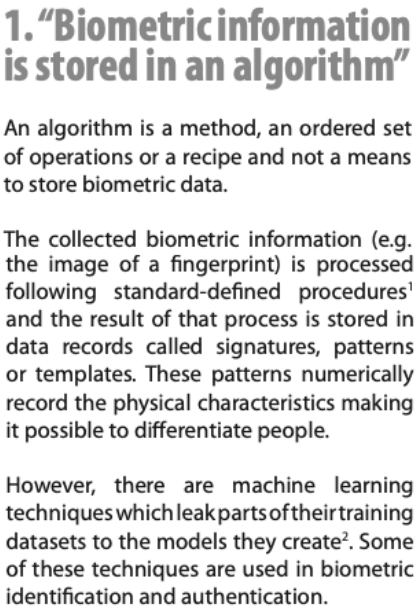
[12] *biometric verification*, which is a standardised term according to Clause 3.8.3 in ISO/IEC 2382-37:2017 is termed *authentication* in the EDPS publication. In order to adhere to the established standard, we use in this paper the term *biometric verification*.

[13] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.8.3

[14] https://eab.org/events/program/166

[15] https://eab.org/events/program/214

are not suitable for general usage, because the data subjects in realistic applications are unknown to the developer of the system. The system behaviour of biometric systems that are applied in realistic applications is that biometric information is stored in a **biometric reference**, meaning *one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison*. This is the definition of a biometric reference in Clause 3.3.16[16] of ISO/IEC 2382-37:2017 [ISO2382-37]. A **biometric template**[17] is indeed one example of such biometric reference, but in other applications like the ICAO 9303 compliant passport, the biometric reference is a **biometric sample**[18]. The biometric reference is a representation of the source and describes a "pattern" contained in the **biometric characteristic**[19]. Furthermore, it is not recommended to call the stored biometric reference a "signature", as the reader might confuse this with signature recognition, as defined in ISO/IEC 19794-7[20].



1. "Biometric information is stored in an algorithm"

An algorithm is a method, an ordered set of operations or a recipe and not a means to store biometric data.

The collected biometric information (e.g. the image of a fingerprint) is processed following standard-defined procedures[1] and the result of that process is stored in data records called signatures, patterns or templates. These patterns numerically record the physical characteristics making it possible to differentiate people.

However, there are machine learning techniques which leak parts of their training datasets to the models they create[2]. Some of these techniques are used in biometric identification and authentication.

Figure 1: Statement "Biometric information is stored in an algorithm", Source: [EDPS2020]

The fact that some machine learning techniques leak information about the training data (which is, for example, an intrinsic property of an autoencoder approach) does not mean that biometric systems in general leak information about the training data, as the publication suggests. It is not because biometric systems may deploy machine learning techniques, that there is leaking from the data [Ross2019].There is in fact no evidence that this is the case.

2. "The use of biometric data is as intrusive as any other identification / authentication system"

The second topic correctly states that biometric data reveals additional personal/sensitive information.

[16] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.16

[17] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.22

[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.21

[19] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.1.2

[20] https://www.iso.org/standard/55938.html

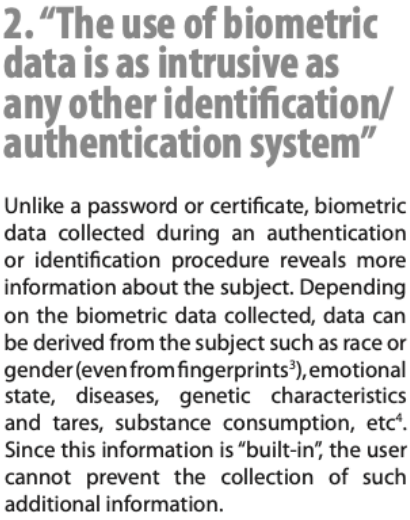


Figure 2: Statement "The use of biometric data is as intrusive as any other identification/authentication system", Source: [EDPS2020]

It is incorrect to state that biometric authentication or identification does imply that data can be derived from the process. Biometric authentication doesn't reveal but processes biometric data. Some personal data can be derived from a leak of the biometric data, which is why biometric templates / references need to be protected.

Both knowledge- and token-based authentication factors have the intrinsic disadvantage that any given security policy can be violated, when the knowledge or the token is forwarded to an unauthorised data subject. On the contrary, biometrics is the only authentication scheme that can establish a secure and unique link between the data subject and the enrolment record.

Taking these two criteria into account, the finding in such benchmark should be revised.

The recommended consequence is to take the best of both worlds and work with privacy enhancing technology (PET) such as the biometric template protection[21] (BTP) methods mandated by ISO/IEC 24745 [ISO24745]. When the biometric references are created based on a BTP concept, then irreversibility, unlinkability, and renewability of biometric references can be guaranteed to a greater degree if not fully. That in turn ensures the protection of the subject's privacy.

Privacy enhancing technologies include also the deployment of smart cards or other tokens for storing biometric references under the control of the data subjects or for biometric comparison on card (ISO/IEC 24787), biometric systems on card (ISO/IEC 17839), or trusted execution environments on mobile or other devices.

3. "Biometric identification / authentication is accurate"

The third statement relates to intra-class variations of biometric features. In other words, by repeating the biometric capture process, the newly created feature vector will in all likelihood not be identical to the previous one, as changes in acquisition conditions (e.g. the illumination or pose of capture subject presenting themselves to the camera) will change the captured facial sample. Similarly, a fingerprint capture process might be influenced by environmental conditions such as temperature or moisture. That part of the statement is correct.

[21] https://de.wikipedia.org/wiki/Biometric_Template_Protection

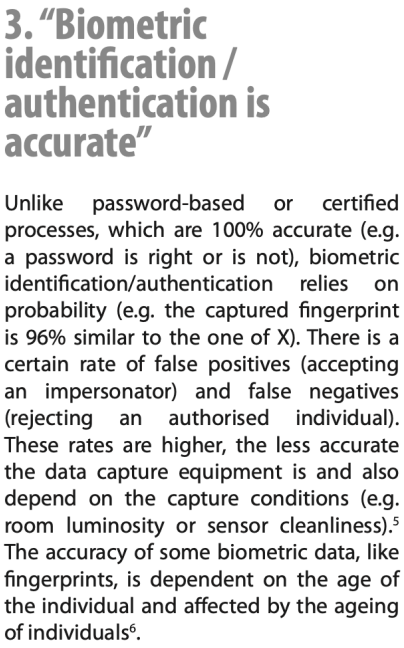


Figure 3: Statement "Biometric identification / authentication is accurate", Source: [EDPS2020]

However, the second part of the statement regarding ageing *("The accuracy of some biometric data (...) individuals")* may be imprecise. While the face as a biometric characteristic is affected by ageing of subjects, we cannot provide an authoritative conclusion regarding other dominant biometric modes. Other biometric characteristics are highly stable. It has been demonstrated by a study of U.S. NIST, that the features extracted from iris (Iris-Codes) are not affected by ageing of the data subject [NIST2015]. Several spectacular (and successful) applications of biometric recognition after a long time exist, and positively influenced the society, for instance, finding Sharbat Gula using her iris patterns after 18 years since she has been portrayed in the National Geographic journal as the "Afghan Girl", as reported by John Daugman[22] - the pioneer of iris recognition. Also for fingerprint recognition studies have shown that a stability of the biometric characteristic over a long period is given [Jain2015] [Galbally2018].

4. "Biometric identification / authentication is precise enough to always differentiate between two people"

The standardised biometric vocabulary ISO/IEC 2382-37:2017 [ISO2382-37] avoids for good reasons the terms "people" or "user" and instead expresses the source of a biometric sample as **biometric data subject**[23] or **biometric capture subject**[24] depending on the context. Furthermore, the term "data subject" is aligned with the terminology in the General Data Protection Regulation (GDPR) and thus should be used in the discussion on biometrics.

[22] https://www.cl.cam.ac.uk/~jgd1000/afghan.html

[23] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.7.5

[24] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.7.3

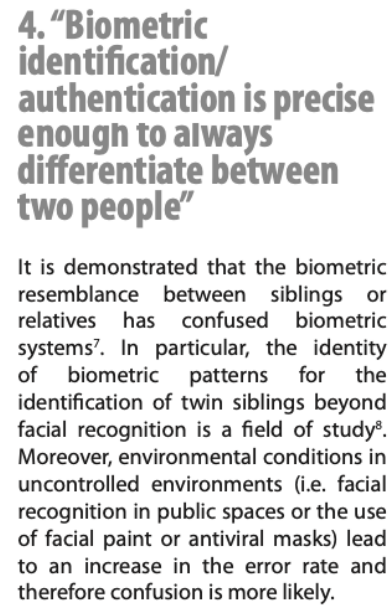


Figure 4: Statement "Biometric identification / authentication is precise enough to always differentiate between two people", Source: [EDPS2020]

Regarding the point that biometric algorithms are challenged to distinguish individuals, it should be emphasised that, when the only source of information is a set of facial images from monozygotic twins, biometric face recognition systems struggle to the same extent as humans with distinguishing between them.

This is why a robust biometric system will utilise multiple types of biometric characteristics, as certain biometric characteristics (e.g. fingerprint or iris) and this will make it possible to distinguish two data subjects with identical genes (monozygotic twins). Such multi-biometric systems (a.k.a. multi-modal biometrics systems) are included in the ISO/IEC TR 24722:2015[25] which describes current practices on multi-biometric fusion [ISO24722].

In addition, as outlined by John Daugman, Iris-Codes can be used to distinguish monozygotic twin siblings[26]. The same is true for fingerprints, if the recognition is based on minutiae comparison, which is the most common method for fingerprint recognition [Jain2002]. A convenient[27] biometric system could, for example, capture the face and two eyes in high resolution – potentially in near infra-red and not in the visible light spectrum – such that the spatial sampling rate of the iris pattern would be sufficient for iris recognition. Thus, a convenient solution for the given problem in this statement is provided. In fact, operational systems already do acquire multi-biometric data. A well-known example is the national ID system in India[28], wherein biometric data from face, iris, and fingerprints has been acquired from nearly the entire Indian population.

Regarding the second part of this statement, it is true that uncontrolled environmental conditions pose a challenge to face recognition systems. Despite those issues, the results of the U.S. NIST Face Recognition Vendor Test (FRVT) indicate the impressive improvement of face recognition systems over the last years [NISTFRVT]. In fact since 2014, error rates for face recognition systems have been reduced significantly, even in large-scale identification scenarios.

[25] https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en

[26] https://www.cl.cam.ac.uk/~jgd1000/genetics.html

[27] „convenient" means compliant to usability standards and designed with the intention to minimise the interaction time

[28] https://www.uidai.gov.in/aadhaar_dashboard/

5. “Biometric identification / authentication is suitable for all people”

For the reader it is not really clear, what the point of criticism is? It is clear that any digital divide in our European society should be avoided. With the same intentions, we should avoid a “biometric divide” meaning that no biometric system should exclude a certain subset of the target population.

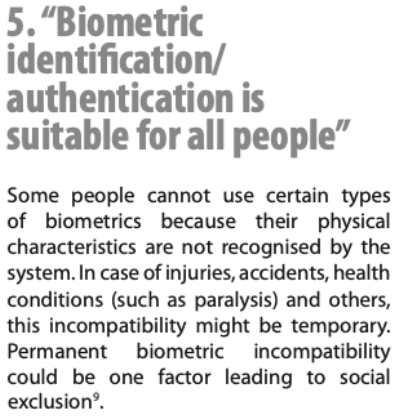


Figure 5: Statement “Biometric identification / authentication is suitable for all people”, Source: [EDPS2020]

For this reason, the ISO/IEC TR 24722:2015 proposes multi-instance (in Clause 2.11) and multi-characteristic-type (in Clause 2.10) biometric systems[29], such that a fall-back procedure can be followed in case a temporary or permanent incompatibility might exist. Such provisions do already exist in operational systems. This is one of the reasons that Aadhaar[30] uses multiple characteristics.

6. “The biometric identification / authentication process cannot be circumvented”

The topic of attacks on **biometric capture devices**[31] is a well justified and an old discussion. Many publications have shown how to lift a fingerprint and subsequently how to generate a fingerprint artefact [Zwie2000], [Marcel2019].

Robustness to attacks is thus fundamental in all non-supervised or semi-supervised applications of biometrics. This risk is covered by the International Standard ISO/IEC 30107-1:2016[32], which elaborates on the taxonomy of presentation attacks (PA) and presentation attack detection (PAD) [ISO30107-1].

[29] https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en

[30] https://uidai.gov.in/

[31] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:sec:3.4.1

[32] http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip

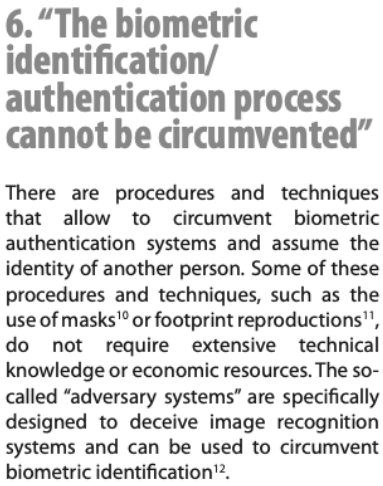


Figure 6: Statement "Biometric identification / authentication process cannot be circumvented", Source: [EDPS2020]

Regarding technical measures for fingerprint recognition systems to be robust to attacks, an overview[33] was given by Sousedik and Busch in [Sous2014]. For face recognition systems, an overview[34] was given by Raghavendra and Busch in [Ragh2017] and for iris recognition one can find an overview in Czajka and Bowyer [Czajka2018] and Marcel et al. [Marcel2019]

Several research projects / programs were devoted to the development of robust presentation attack detection (PAD) for face, iris, and fingerprint recognition and have been conducted recently:

- Tabula Rasa[35]
- BEAT[36]
- SWAN[37]
- ODIN[38]

The biometric community is also strongly committed to creating independent and open-to-the-public platforms for benchmarking biometric technology (i.e. presentation attack detection mechanisms). As an example, the LivDet series[39] evaluates presentation attack detection methods for fingerprint recognition[40] and for iris recognition[41].

These research activities have significantly improved robustness of biometric capture devices. Moreover, the robustness can now be quantifiably tested and certified based on the International Standard ISO/IEC 30107-3[42] which provides the corresponding testing metrics and methodology [ISO30107-3]. We can safely conclude that testing of PAD mechanism with regards to the strength of function with presentation attack instruments that are of significant attack potential is cost intensive but needed, especially when unsupervised operation of biometric capture devices is intended. In this context, the German Federal Office for Information Security (BSI) established a biometric evaluation centre in order to test biometric capture devices for their capability in presentation attack

[33] http://digital-library.theiet.org/deliver/fulltext/iet-bmt/3/4/IET-MT.2013.0020.pdf?itemId=/content/journals/10.1049/iet-bmt.2013.0020&mimeType=pdf&isFastTrackArticle=

[34] http://dl.acm.org/ft_gateway.cfm?id=3038924&ftid=1858951&dwn=1&#URLTOKEN#

[35] http://www.tabularasa-euproject.org/project

[36] https://www.beat-eu.org/

[37] https://www.ntnu.edu/iik/swan/

[38] https://www.iarpa.gov/index.php/research-programs/odin

[39] http://livdet.org/

[40] since nine editions, with the most recent available at https://livdet.diee.unica.it

[41] since four editions, with the most recent available at http://www.iris2020.livdet.org

[42] https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en

detection. It should be noted that recently a Protection Profile for biometric enrolment and verification for unlocking a device was published [PP2020]. We therefore suggest and recommend, to add to this statement that biometric systems should – as state of the art - provide measures to detect such adversarial behaviour, such as deploying PAD-tested capture devices, in particular for unsupervised capture environments.

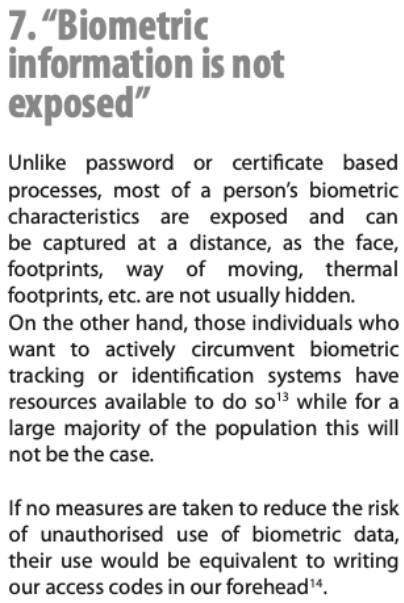
7. "Biometric information is not exposed"

It is true that the face of a data subject is exposed to the public and can be captured even at a distance in a non-cooperative manner (i.e. without consent of the **biometric capture subject**[43]).

This specifically relates to facial images which are captured by video surveillance systems as described in ISO/IEC 30137-1:2019[44] [ISO30137-1]. Thus, from a technical perspective it seems self-contradicting that the GDPR has formulated an exemption in recital 51 from the definition and the requirements set forth by GDPR Article 9.1:

"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. (…)"

However, for forensic applications, like the investigations of the terrorist attacks at Brussels-Airport[45] or at the Breitscheidplatz[46] in Berlin, it is to the benefit of our European society that such exposed biometric characteristics can indeed be acquired without cooperation of the capture subject.



7. "Biometric information is not exposed"

Unlike password or certificate based processes, most of a person's biometric characteristics are exposed and can be captured at a distance, as the face, footprints, way of moving, thermal footprints, etc. are not usually hidden.
On the other hand, those individuals who want to actively circumvent biometric tracking or identification systems have resources available to do so[13] while for a large majority of the population this will not be the case.

If no measures are taken to reduce the risk of unauthorised use of biometric data, their use would be equivalent to writing our access codes in our forehead[14].

Figure 7: Statement "Biometric information is not exposed", Source: [EDPS2020]

From a technical perspective, a system operator (or a legislative body) can always give preference to a biometric system that cannot be attacked with biometric samples that have been captured without consent of the data subject, if that is the intention of the statement. If desired, preference should be given to other biometric characteristics that definitely don't have this drawback, as the biometric characteristic can *only* be captured when the data subject is

[43] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.7.3

[44] https://www.iso.org/obp/ui/#iso:std:iso-iec:30137:-1:ed-1:v1:en

[45] https://en.wikipedia.org/wiki/2016_Brussels_bombings

[46] https://en.wikipedia.org/wiki/2016_Berlin_truck_attack

being aware of the capture process, for instance vascular patterns [Uhl2020] based on ISO/IEC 19794-9 or ISO/IEC 39794-9.

As an alternative with less robustness one could deploy an iris recognition system based on ISO/IEC 19794-6 or ISO/IEC 39794-6, if the spectral band is e.g. in the range of 1150 to 1350 nm and thus the biometric characteristic is not observable from the outside without a dedicated capture device [Ross2009].

It is unlikely that either of these two biometric characteristics can be captured without the data subject being aware of the capture process.

The last paragraph in this topic is overcome by events and technological advancements of face recognition systems, thus potentially misleading the reader. A facial photo as captured by a video surveillance system or taken from the internet would have been sufficient to attack a face capture device 20 years ago. However, today's face capture devices like those installed in the Automatic Border Control Gates at Schengen border control processes will detect a printout or display attack as described by Raghavendra [Ragh2017]. Still today, some low-cost mobile devices can be attacked by such low-level artefacts. Nevertheless, more advanced 3D face recognition technology like the mechanism embedded in the Face ID[47] cannot be fooled by any presentation attack instrument derived from surveillance video footage. For testing such robustness, please refer to our explanation in the previous section.

We therefore suggest and recommend, to add to and complete this statement that measures are needed to restrict the use and to protect biometric information, including by legislative initiatives.

8. "Any biometric processing involves identification / authentication"

This statement uses an interpretation of biometric processing that is too wide. Biometric processing is solely to be performed with the purpose of biometric recognition. Processing of personal physiological data with other objectives is not to be considered biometric processing.

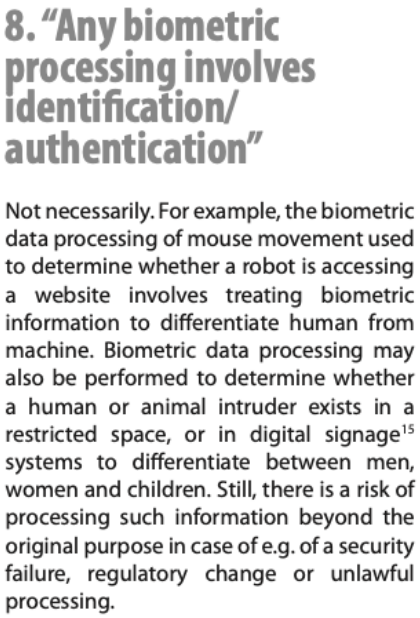


Figure 8: Statement "Any biometric processing involves identification / authentication", Source: [EDPS2020]

In our technical understanding, a function creep might be possible in a biometric system, as well as in a non-biometric system. However, the GPDR in Article 13.3 clearly limits the controller to use the data only for the original purpose: „… *in case he intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose ...*"

Thus, the function creep as indicated in the statement would be an unlawful processing and subject to the fining rules.

We therefore suggest and recommend, to add to and complete this statement by stating that biometric systems should be used with well-defined purposes and that they are not limited to use for identification or verification, but could also be used to categorize.

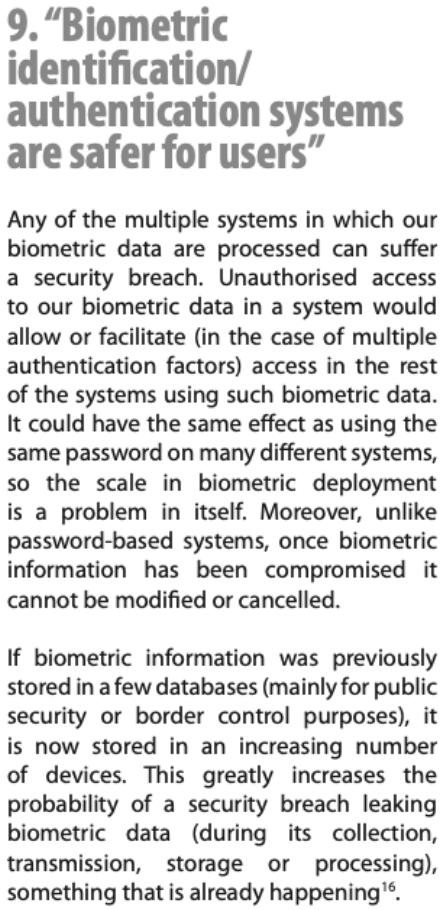
[47] https://en.wikipedia.org/wiki/Face_ID

9. "Biometric identification / authentication systems are safer for users"

While a central system is more likely to be attacked than many personal storage devices, a central system is also likely to be better protected than many personal storage devices. The same holds true for central systems with personal biometric data. So far, the statement is correct.

But the claim that with a biometric system one may *"… have the same effect as using the same password on many different systems ...*" the authors neglect the requirement of ISO/IEC 24745 [ISO24745], which demands in Clause 5.2.3 "*independent references across different applications*", in order to have a countermeasure against the "cross-database-comparison" threat described in Clause 6.1: "*Biometric references may be used to link subjects across different applications in the same database or across different databases. Privacy is related to the unlinkability of the stored biometric reference"* [ISO24745].

Since more than ten years now such systems are available. A significant progress towards biometric template protection in general and renewability specifically was achieved in the European TURBINE project[48] in the years 2008 until 2011. When the biometric references are created based on a BTP concept, then irreversibility, unlinkability, and renewability of biometric references can be guaranteed.



9. "Biometric identification/ authentication systems are safer for users"

Any of the multiple systems in which our biometric data are processed can suffer a security breach. Unauthorised access to our biometric data in a system would allow or facilitate (in the case of multiple authentication factors) access in the rest of the systems using such biometric data. It could have the same effect as using the same password on many different systems, so the scale in biometric deployment is a problem in itself. Moreover, unlike password-based systems, once biometric information has been compromised it cannot be modified or cancelled.

If biometric information was previously stored in a few databases (mainly for public security or border control purposes), it is now stored in an increasing number of devices. This greatly increases the probability of a security breach leaking biometric data (during its collection, transmission, storage or processing), something that is already happening[16].

Figure 9: Statement "Biometric identification / authentication are safer for users", Source: [EDPS2020]

At the end of the TURBINE project (in the year 2011), the EDPS has issued an opinion[49] about biometric template protection in general and the pseudo-identities (as the protected references are named in TURBINE and later in ISO/IEC 24745) specifically. The positive assessment indicated in Clause 2.1.3: "*The Turbine project described a procedure whereby the pseudo-identities can be revoked. With such a solution, the data subject shall have alternative means for authentication for the services when the pseudo-identities need to be revoked. … Moreover, the revocability of the template ensures that the accuracy of the data is preserved (Article 4.1.d of Regulation 45/2001). If the data is no longer accurate (compromised, etc), the possibility to revoke and renew the template based on biometric data allows the data to be kept up to date."*

[48] https://cordis.europa.eu/project/id/216339

[49] https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf

Furthermore, the concept of biometric template protection has not only been adopted ISO/IEC 24745, which has reached global attention, but it was also included in the NIST Special Publication 800-63B[50].

Following the TURBINE project, two further European projects namely FIDELITY[51] and SWAN[52] further developed biometric template protection mechanisms.

A result of that research was the Bloom filter-based approach [Rathg2013], [Rathg2014], which can provide unlinkable, irreversible, and renewable pseudo-identities at no loss of biometric recognition performance. The formal proof on the security properties was given in the work of Gomez-Barrero [Gomez2018]. Numerous other biometric template protection methods which achieve those goals have been developed since.

We therefore suggest and recommend, to add to and complete this statement with a reference to ISO/IEC 24745 and to the recent state of the art on BTP.

10. "Biometric authentication is strong"

The statement that two authentication factors are stronger than one authentication factor is generally true. The relevant European biometric systems already utilize multi-factor authentication.

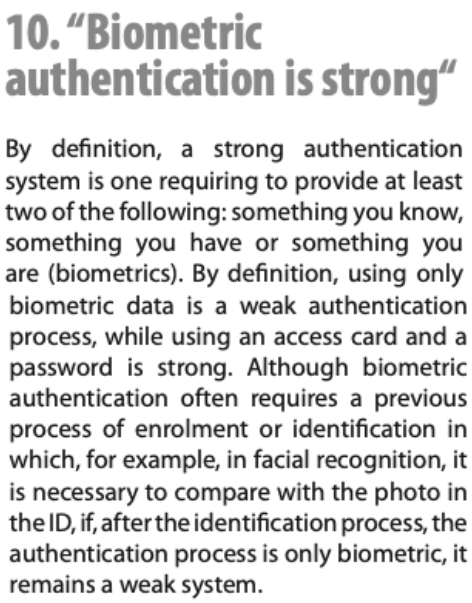


Figure 10: Statement "Biometric authentication is strong",
Source: [EDPS2020]

For example, in the border control processes at the Schengen borders, one authentication factor is the passport of the traveller, the second authentication factor is the facial biometric characteristic, and the third authentication factor is the index finger (under assumption, we would extend the above definition and consider the fingerprint pattern of a data subject mutually independent from the face).

Similarly, in the Visa Information system the first authentication factor is possession (of the sticker with the visa-ID) and the second to the eleventh authentication factor are the ten fingerprint instances. In this context the entropy discussion above is also relevant.

We therefore suggest and recommend, to add to and complete this statement that biometric systems shall rely on multi-factor authentication, in other words shall combine a biometric comparison (based on what you are) with something you have or know.

11. "Biometric identification / authentication is more user-friendly"

The statement in some sense contradicts the previous statement, as less security (meaning only one biometric authentication factor) implicitly results in increased security: Biometric characteristics can neither be lost (like an access token) nor forgotten (like a password).

[50] https://pages.nist.gov/800-63-3/sp800-63b.html

[51] https://cordis.europa.eu/project/rcn/102324/factsheet/en

[52] https://www.ntnu.edu/iik/swan/

Figure 11: Statement "Biometric identification / authentication is more user-friendly", Source: [EDPS2020]

In most practical systems, the biometric claim is submitted as a token (e.g. the passport of the traveller), which then initiates the verification process.

In case of multi-factor authentication systems, one cannot by nature of biometrics state that biometric recognition is per se user-friendly or user-unfriendly. It all depends on whether the system design is compliant to the requirements in the International Standard ISO 9241-11:2018[53] on ergonomics of human-system interaction. The same holds true for other authentication mechanisms.

12. "Biometric information converted to a hash is not recoverable"

The cryptographic concept of a "hash" is not applicable to biometric references due to the intra-class variation explained above.

The BioHash mechanism is just one example of transforming a biometric template into a protected biometric reference and by no means representative for the variety of BTP approaches. In addition, we would like to highlight again that the BioHash mechanism is just one way of transforming a biometric template into a protected biometric reference, which may not achieve a top performance in terms of privacy protection and security in a benchmark with other BTP technologies [ISO30136], [Gomez2018]. We can agree that some published BTP schemes are of insufficient security and grant no irreversibility.

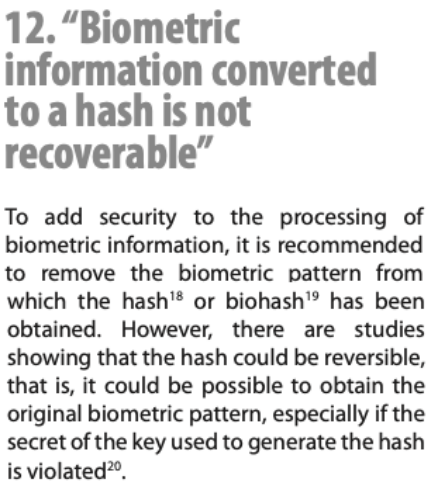


Figure 12: Statement "Biometric information converted to a hash is not recoverable", Source: [EDPS2020]

On the other hand, research has shown that by fulfilling the requirements of ISO/IEC 24745 [ISO24745], secure template protection is possible: More recent approaches, such as the Bloom filter-based method by Rathgeb et al.

[53] https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

[Rathg2014] in its modified version of [Gomez2016] have been validated to prevent reconstruction of a biometric sample. Furthermore, that enhanced cascaded Bloom filter approach does not allow any recovering [Gomez2016].

More recently, the progress of homomorphic encryption (HE) has validated the assumption that comparison of pseudonymous identities is possible in the HE domain as shown by recent work [Bodetti2018] [Gomez2017], [Drozd2019b] and [Kolb2019]. This kind of approaches counts with rigorous mathematical proofs, stemming from the mathematical and cryptographic communities, which support the desired irreversibility, unlinkability, and renewability properties of biometric pseudonymous identifiers.

13. "Stored biometric information does not allow the original biometric information to be reconstructed from which it has been extracted"

To the reader it is not very clear, how this statement differs from the previous statement. It is true that iris samples can be reconstructed from Iris-Codes [Gomez2017], fingerprint samples can be reconstructed from minutiae templates [Cappelli2007], and face images can be reconstructed from latent neural network representations [Mai2018].

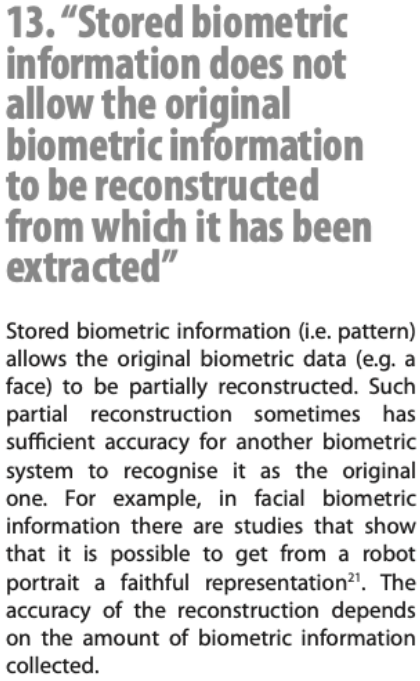


Figure 13: Statement "Stored biometric information does not allow the original biometric information to be reconstructed from which it has been extracted",
Source: [EDPS2020]

However, these attacks expect the biometric template to be available in plaintext in order to reconstruct a biometric sample. As already stated in previous sections, these attacks are not possible for ISO/IEC 24745 compliant BTP systems. Thus this risk assessment was one of the driving reasons to develop the Bloom filter-based approach by Rathgeb et al. [Rathg2014] in order to prevent a reconstruction of a biometric sample from the stored reference [Gomez2020]. Numerous other biometric template protection methods which achieve this goal have been developed since.

14. "Biometric information is not interoperable"

This statement correctly confirms that biometric standards exist. Since the inauguration of international standardisation committee devoted to biometrics (ISO/IEC JTC1 SC37)[54], numerous standards have been developed.

[54] https://committee.iso.org/home/jtc1sc37

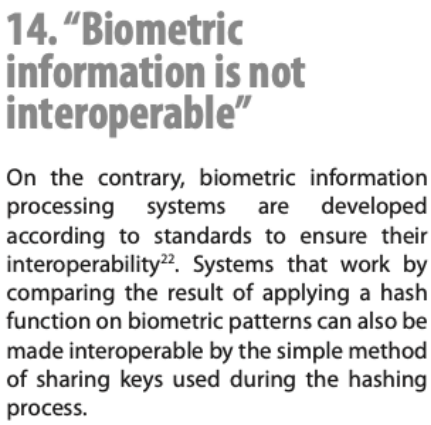


Figure 14: Statement "Biometric information is not interoperable", Source: [EDPS2020]

Some system operators prefer, to implement a system based on proprietary format for data records and interfaces. That is a high-risk strategy, as a vendor-lock-in may have dramatic impacts.

On the contrary, other operators have agreed upon an open biometrics system, which allows and requires the exchange of standardised reference data. Those systems can be designed based on the standards provided by ISO/IEC JTC1 SC37. We therefore suggest and recommend, to refer to the most important standards of SC37.

Conclusion

EAB, as a non-profit, non-partisan association, supports a transparent, comprehensive, fact-based and open-ended discussion on biometrics. Biometrics will continue to have a strong impact on the security of European borders and other governmental and commercial applications. Biometrics play a crucial role in such processes. In order to stay compliant with European data protection principles, in particular those confirmed in the GDPR, Privacy Enhancing Technology that has been researched, developed, used and is available should be advanced and deployed. As all technology, biometric technology should be carefully implemented, tested, and certified equally. A pro-active and cognizant approach based on the latest research and developments presenting state of the art could foster awareness among the citizens and policymakers, as well as contribute to minimising potential negative effects and perception of biometric technology and innovation by individuals and society as a whole. In order to clarify the discussion, it is important to keep the technical and policy issues clearly separated. The European Commission is invited to support research and development, industrial follow ups as the adoption and deployment of ISO/IEC standards [ISO19794-1], [ISO39794-1] as well as the interaction with the European Association for Biometrics.

In view of the importance of the current topics and challenges covered, the EAB invites EDPS and aepd to contact EAB, to create a joint position paper together with the European Association for Biometrics.

References

[Bodetti2018] V. Boddeti: "Secure Face Matching Using Fully Homomorphic Encryption", in Proceedings BTAS, 2018

[Buchmann2014] N. Buchmann, C. Rathgeb, H. Baier, C. Busch: "Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area", in Proceedings of the Annual Privacy Forum (APF), May 20-21, Athens, Greece, 2014

[Cappelli2007] R. Cappelli, D. Maio, A. Lumini, D. Maltoni: "Fingerprint Image Reconstruction From Standard Templates", in IEEE Trans. on Pattern Analysis and Machine Intelligence, 2007

[Czajka2018] A. Czajka, K. Bowyer: "Presentation Attack Detection for Iris Recognition: An Assessment of the State-of-the-Art", in ACM Computing Surveys, 2018

[Drozd2019a] P. Drozdowski, C. Rathgeb, C. Busch: "Computational Workload in Biometric Identification Systems: An Overview", in IET Biometrics, 2019

[Drozd2019b] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, C. Busch: "On the Application of Homomorphic Encryption to Face Identification", in Proceedings of the IEEE 18th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 18-20, 2019

[EDPS2020] EDPS and AEPD: "14 Misunderstandings with regard to Biometric Identification and Authentication", online at: https://edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf, accessed July, 2020

[Galbally2018] J. Galbally, R. Haraksim, L. Beslay: "A Study of Age and Ageing in Fingerprint Biometrics", in IEEE Transactions on Information Forensics and Security (TIFS), pp(99):1-1, 2018

[Gomez2016] M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch, J. Fierrez: "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters", in Journal Information Sciences, 370-371, Elsevier, 2016

[Gomez2017] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez: "Multi-biometric template protection based on Homomorphic Encryption", in Journal Pattern Recognition, Elsevier, 2017

[Gomez2018] M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch: "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems", in IEEE Transactions on Information Forensics and Security (TIFS), 2018

[Gomez2020] M. Gomez-Barrero, J. Galbally: "Reversing the irreversible: A survey on inverse biometrics", in Journal Computers & Security, Elsevier, 2020

[ISO19794-5] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 19794-5:2005, Biometric data interchange format - Part 5: Face image data, 2005.

[ISO2382-37] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37, Information technology – Vocabulary – Part 37: Biometrics, 2017.

[ISO24722] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 24722, Multimodal and other multibiometric fusion, 2015.

[ISO24745] ISO/IEC JTC1 SC27 Security techniques, ISO/IEC 24745:2011, Biometric information protection, 2011.

[ISO29794-1] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 29794-1:2016, Biometric sample quality – Part 1: Framework, 2016.

[ISO39794-1] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 39794-1:2019, Extensible biometric data interchange format – Part 1: Framework, 2019.

[ISO30107-1] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3:2017, Biometric presentation attack detection – Part 1: Framework, 2016.

[ISO30107-3] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3:2017, Biometric presentation attack detection – Part 3: Testing and Reporting, 2017.

[ISO30137-1] ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30137-1:2019, Use of biometrics in video surveillance systems – Part 1: System design and specification, 2019.

[ICAO9303] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents - Part 9: Deployment of Bio-metric Identification and Electronic Storage of Data in MRTDs (7th edition), 2015.

[Jain2002] A. Jain, S. Prabhakar, S. Pankanti: "On the similarity of identical twin fingerprints", in Pattern Recognition, Volume 35, Issue 11, Pages 2653-266, 2002

[Jain2015] S. Yoon and A. Jain: "Longitudinal study of fingerprint recognition", in Proceedings of the National Academy of Sciences (PNAS), vol. 112, no. 28, 2015

[Kolb2019] J. Kolberg, P. Bauspieß, M. Gomez-Barrero, C. Rathgeb, M. Dürmuth, C. Busch: "Template Protection based on Homomorphic Encryption: Computational Efficient Application to Iris-Biometric Verification and Identification ", in Proceedings of IEEE International Workshop on Information Forensics and Security 2019 (WIFS 2019), Delft, NL, December 9-12, 2019

[Mai2018] G. Mai, K. Cao, P. C. Yuen, A. K. Jain: “On the Reconstruction of Face Images from Deep Face Templates”, in IEEE Trans. on Pattern Analysis and Machine Intelligence, 2018

[Marcel2019] S. Marcel, M- Nixon, J. Fierrez, N. Evans: "Handbook of Biometric Anti-Spoofing", Springer, 2019

[NIST2015] P. Grother, J. Matey, G. Quinn: " IREX VI: Mixed-effects Longitudinal Models for Iris Aging", 2015

[NISTFRVT] U.S. NIST Face Recognition Vendor Test

[PP2020] Biometrics Security iTC, Biometric Protection Profile, https://biometricitc.github.io/

[Ragh2017] R. Raghavendra, C. Busch: "Presentation Attack Detection methods for Face Recognition System - A Comprehensive Survey", in ACM Computing Surveys, 2017

[Rathg2013] C. Rathgeb, F. Breitinger, C. Busch: "Alignment-Free Cancelable Iris Biometric Templates based on Adaptive Bloom Filters", in Proceedings of the 6th IAPR International Conference on Biometrics (ICB 2013), June 4-7, Madrid, 2013

[Rathg2014] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), 2014

[Ross2009] A. Ross. R. Pasula, L. Hornak: "Exploring Multispectral Iris Recognition beyond 900nm", in Proceedings of 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2009

[Ross2019] A. Ross: "Some Research Problems in Biometrics: The Future Beckons", in Proceedings of 12th International Conference on Biometrics (ICB), 2019

[Sous2014] C. Sousedik, C. Busch: "Presentation attack detection methods for fingerprint recognition systems: a survey", in Journal on Biometrics, IET, 2014

[Uhl2020] A. Uhl, C. Busch, S. Marcel, R. Veldhuis: "Handbook of Vascular Biometrics", Springer, 2020

[Zwie2000] A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems" In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, 2000