








## POSITION PAPER

# A response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics

Christoph Busch<sup>1,2</sup>  | Adam Czajka<sup>3</sup>  | Farzin Deravi<sup>4</sup>  | Pawel Drozdowski<sup>1</sup>  |  
 Marta Gomez-Barrero<sup>5</sup> | Georg Hasse<sup>6</sup> | Olaf Henniger<sup>7</sup> | Els Kindt<sup>8</sup> |  
 Jascha Kolberg<sup>1</sup>  | Alexander Nouak<sup>7,9</sup> | Kiran Raja<sup>10</sup> |  
 Raghavendra Ramachandra<sup>10</sup>  | Christian Rathgeb<sup>1</sup>  | Jean Salomon<sup>9</sup> |  
 Raymond Veldhuis<sup>11</sup>

<sup>1</sup>Department of Computer Science, Hochschule Darmstadt, Darmstadt, Germany

<sup>2</sup>Norwegian Biometrics Laboratory (NBL), Norwegian University of Science and Technology, Gjøvik, Norway

<sup>3</sup>Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, Indiana, USA

<sup>4</sup>School of Engineering and Digital Arts, University of Kent, Canterbury, UK

<sup>5</sup>Hochschule Ansbach, Ansbach, Germany

<sup>6</sup>Secunet, Essen, Germany

<sup>7</sup>Fraunhofer IGD, Darmstadt, Germany

<sup>8</sup>KU Leuven, Leuven, Belgium

<sup>9</sup>European Association for Biometrics, Darmstadt, Germany

<sup>10</sup>Department of IIK, Norwegian University of Science and Technology, Gjøvik, Norway

<sup>11</sup>Department of EECMS, University of Twente, Enschede, The Netherlands

### Correspondence

Christoph Busch, Hochschule Darmstadt,  
Haardtring 100, 64295 Darmstadt, Germany.  
Email: [Christoph.Busch@ntnu.no](mailto:Christoph.Busch@ntnu.no)

### Abstract

The intention of this position paper is to comment on the joint European Data Protection Supervisor (EDPS)-Agencia Española de Protección de Datos (aepd) publication '14 Misunderstandings with regard to Biometric Identification and Authentication' that was published in June 2020 and to provide additional input to help with the better understanding of the issues raised in that publication. In particular, it aims to highlight some important missing information in the aforementioned publication. It is hoped that this paper will help with any future revision of 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, border control, face recognition, vulnerability analysis

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2021 European Association for Biometrics (EAB). *IET Biometrics* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

## 1 | 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’.<sup>1</sup> The paper looks at biometric identification and verification<sup>2,3</sup> and specifically focuses on fingerprint and face recognition. The misunderstandings listed in the white paper are presented as popular beliefs currently held by the society and emerging from the recent rise in the applications of biometric technologies. The paper proceeds to present and then dismiss each of these assertions in turn to highlight the shortcomings and weaknesses of these technologies.

Interested stake holders have been studying the vulnerabilities of biometric technologies addressed in the White Paper and their possible countermeasures for a long time. We definitely agree that biometric technologies are no universal panacea for security and identity needs of the society, but require a 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, non-partisan association. The EAB’s mission is to tackle the complex challenges faced by 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 organise, 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,<sup>4</sup> and online meetings.<sup>5</sup> It is in this spirit that the EAB has reviewed the afore-mentioned publication and discussed with its members all the 14 topics addressed therein. We feel that the arguments in the white paper as well as the referenced literature are incomplete and therefore provide the information below with the intention to contribute to and to complement it.

In the remainder of the paper, some of the key ‘misunderstandings’ listed in the white paper that require elaboration are highlighted in separate sections. Alongside the statement by the white paper in each case, additional explanatory information and references are provided. Finally, a concluding section is provided to summarise the overall contributions of this paper.

## 2 | BIOMETRIC INFORMATION IS STORED IN AN ALGORITHM

EDPS-Statement 1:

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 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. Some of these techniques are used in biometric identification and authentication. Source: [1].

It is true that certain biometric recognition 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 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<sup>6</sup> of ISO/IEC 2382-37:2017 [2]. A **biometric template**<sup>7</sup> 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**.<sup>8</sup> The biometric reference is a representation of the source and describes a ‘pattern’ contained in the **biometric characteristic**.<sup>9</sup> 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.<sup>10</sup>

<sup>1</sup>[https://edps.europa.eu/sites/edp/files/publication/joint\\_paper\\_14\\_misunderstandings\\_with\\_regard\\_to\\_identification\\_and\\_authentication\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_authentication_en.pdf).

<sup>2</sup>*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*.

<sup>3</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.8.3>.

<sup>4</sup><https://eab.org/events/program/166>.

<sup>5</sup><https://eab.org/events/program/214>

<sup>6</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.16>.

<sup>7</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.22>.

<sup>8</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.3.21>.

<sup>9</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.1.2>.

<sup>10</sup><https://www.iso.org/standard/55938.html>.

The fact that some machine learning techniques leak information about the training data (which is, e.g. an intrinsic property of an autoencoder approach) does not mean that biometric systems in general leak information about the training data, as may be inferred from the statement above. It is not because biometric systems may deploy machine learning techniques, but that there is leaking from the data [3]. There is in fact no evidence that this is the case.

### 3 | THE USE OF BIOMETRIC DATA IS AS INTRUSIVE AS ANY OTHER IDENTIFICATION/AUTHENTICATION SYSTEM

EDPS-Statement 2:

Unlike a password or certificate, biometric data collected during an authentication or identification procedure reveals more information about the subject. Depending on the biometric data collected, data can be derived from the subject such as race or gender (even from fingerprints), emotional state, diseases, genetic characteristics and tares, substance consumption, etc. Since this information is 'built-in', the user cannot prevent the collection of such additional information. Source: [1].

It is inaccurate to state that biometric authentication or identification does imply that additional personal data can be derived from the process. Biometric authentication does not reveal but processes biometric data, while assuming that the biometric capture process was conducted with a trusted capture device, which is not going to unlawfully share or sell the data to a third party. After processing, reference data is stored and personal data can be derived from a leak of the biometric reference data, which is why biometric templates/references need to be protected.

Both knowledge-based 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.

The recommended consequence is to incorporate PET such as the biometric template protection<sup>11</sup> (BTP) methods mandated by ISO/IEC 24745 [4]. 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 also include 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.

### 4 | BIOMETRIC IDENTIFICATION/AUTHENTICATION IS PRECISE ENOUGH TO ALWAYS DIFFERENTIATE BETWEEN TWO PEOPLE

EDPS-Statement 4:

It is demonstrated that the biometric resemblance between siblings or relatives has confused biometric systems. In particular, the identity of biometric patterns for the identification of twin siblings beyond facial recognition is a field of study. Moreover, environmental conditions in uncontrolled environments (i.e. facial recognition in public spaces or the use of facial paint or antiviral masks) lead to an increase in the error rate and therefore confusion is more likely. Source: [1].

The standardised biometric vocabulary ISO/IEC 2382-37:2017 [2] avoids for good reasons the terms 'people' or 'user' and instead expresses the source of a biometric sample as **biometric data subject**<sup>12</sup> or **biometric capture subject**<sup>13</sup> 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.

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 when 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<sup>14</sup> which describes current practices on multi-biometric fusion [5].

In addition, as outlined by John Daugman, Iris-Codes can be used to distinguish monozygotic twin siblings.<sup>15</sup> The same

<sup>11</sup>[https://de.wikipedia.org/wiki/Biometric\\_Template\\_Protection](https://de.wikipedia.org/wiki/Biometric_Template_Protection).

<sup>12</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382-37:ed-2:v1:en:term:3.7.5>.

<sup>13</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382-37:ed-2:v1:en:term:3.7.3>.

<sup>14</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en>.

<sup>15</sup><https://www.cl.cam.ac.uk/~jgd1000/genetics.html>.

is true for fingerprints, if the recognition is based on minutiae comparison, which is the most common method for fingerprint recognition [6]. A convenient<sup>16</sup> 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,<sup>17</sup> 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. National Institute of Standards and Technology (NIST) Face Recognition Vendor Test indicate the impressive improvement of face recognition systems over the last years [7]. In fact, since 2014, error rates for face recognition systems have been reduced significantly, even in large-scale identification scenarios.

## 5 | THE BIOMETRIC IDENTIFICATION/AUTHENTICATION PROCESS CANNOT BE CIRCUMVENTED

EDPS-Statement 6:

There are procedures and techniques that allow to circumvent biometric authentication systems and assume the identity of another person. Some of these procedures and techniques, such as the use of masks or footprint reproductions, do not require extensive technical knowledge or economic resources. The so-called ‘adversary systems’ are specifically designed to deceive image recognition systems and can be used to circumvent biometric identification. Source:[1].

The topic of attacks on **biometric capture devices**<sup>18</sup> is a well justified and an old discussion. For instance, many publications have shown how to lift a fingerprint and subsequently how to generate a fingerprint artefact [8, 9].

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,<sup>19</sup> which elaborates on the taxonomy of presentation attacks (PA) and PA detection (PAD) [10].

Regarding technical measures for fingerprint recognition systems to be robust to attacks, an overview<sup>20</sup> was given by Sousedik and Busch in Ref.[11]. For face recognition systems, an overview<sup>21</sup> was given by Raghavendra and Busch in Ref. [12]; and for iris recognition, one can find an overview in Czajka and Bowyer [13] and Marcel et al. [9].

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

- Tabula Rasa<sup>22</sup>
- BEAT<sup>23</sup>
- SWAN<sup>24</sup>
- ODIN<sup>25</sup>

The biometric community is also strongly committed to creating independent and open-to-the-public platforms for benchmarking biometric PAD mechanisms. As an example, the LivDet series<sup>26</sup> evaluates PAD methods for fingerprint recognition<sup>27</sup> and for iris recognition.<sup>28</sup>

These research activities have significantly improved the robustness of biometric capture devices. Moreover, the robustness can now be quantifiably tested and certified based on the International Standard ISO/IEC 30107-3<sup>29</sup> which provides the corresponding testing metrics and methodology [14]. We can safely conclude that testing of PAD mechanisms with regards to the strength of function of PA instruments that are of significant attack potential can be costly but needed, especially when unsupervised operation of biometric capture devices is intended. In this context, the German Federal Office for Information Security, and Bundesamt für Sicherheit in der Informationstechnik established a biometric evaluation centre in order to test biometric capture devices for their capability of PAD. It should be noted that recently a Protection Profile for biometric enrolment and verification for unlocking a device was published [15]. We, therefore, suggest and recommend to add to this statement that biometric systems should provide measures to detect such adversarial behaviour, such as deploying PAD-tested capture devices, particularly for unsupervised capture environments.

## 6 | BIOMETRIC INFORMATION IS NOT EXPOSED

EDPS-Statement 7:

<sup>20</sup><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=>

<sup>21</sup>[http://dl.acm.org/ft\\_gateway.cfm?id=3038924&ftid=1858951&dwn=1&#URLTOKEN](http://dl.acm.org/ft_gateway.cfm?id=3038924&ftid=1858951&dwn=1&#URLTOKEN).

<sup>22</sup><http://www.tabularasa-euproject.org/project>.

<sup>23</sup><https://www.beat-eu.org/>.

<sup>24</sup><https://www.ntnu.edu/iik/swan/>.

<sup>25</sup><https://www.iarpa.gov/index.php/research-programs/odin>.

<sup>26</sup><http://livdet.org/>.

<sup>27</sup>Since nine editions, with the most recent available at <https://livdet.dice.unica.it>.

<sup>28</sup>Since four editions, with the most recent available at <http://www.iris2020.livdet.org>.

<sup>29</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v:1:en>.

<sup>16</sup>‘convenient’ means compliant to usability standards and designed with the intention to minimise the interaction time.

<sup>17</sup>[https://www.uidai.gov.in/aadhaar\\_dashboard/](https://www.uidai.gov.in/aadhaar_dashboard/).

<sup>18</sup><https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v:1:en:sec:3.4.1>.

<sup>19</sup>[http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227\\_ISO\\_IEC\\_30107-1\\_2016.zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip).

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 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. Source: [1].

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**).<sup>30</sup>

This specifically relates to facial images which are captured by video surveillance systems as described in ISO/IEC 30137-1:2019<sup>31</sup> [16]. 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<sup>32</sup> or at the Breitscheidplatz<sup>33</sup> 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.

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 desired, preference should be given to other biometric characteristics that definitely do not have this drawback, as the biometric characteristic can *only* be captured when the data subject is being aware of the capture process, for instance, vascular patterns [17] 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, for example, in the range of 1150–1350 nm and thus the biometric characteristic is not observable from the outside without a dedicated capture device [18].

It is unlikely that neither vascular patterns nor near infrared iris patterns can be captured without the data subject being aware of the capture process.

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 [12]. Even today, some low-cost mobile devices can be attacked by such low-quality artefacts. Nevertheless, more advanced 3D face recognition technology like the mechanism embedded in the Face ID<sup>34</sup> cannot be fooled by any PA instrument derived from surveillance video footage. For testing such robustness, please refer to our explanation in the previous section.

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

## 7 | BIOMETRIC IDENTIFICATION/AUTHENTICATION SYSTEMS ARE SAFER FOR USERS

EDPS-Statement 9:

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

<sup>30</sup> <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.7.3>.

<sup>31</sup> <https://www.iso.org/obp/ui/#iso:std:iso-iec:30137:-1:ed-1:v1:en>.

<sup>32</sup> [https://en.wikipedia.org/wiki/2016\\_Brussels\\_bombings](https://en.wikipedia.org/wiki/2016_Brussels_bombings).

<sup>33</sup> [https://en.wikipedia.org/wiki/2016\\_Berlin\\_truck\\_attack](https://en.wikipedia.org/wiki/2016_Berlin_truck_attack).

<sup>34</sup> [https://en.wikipedia.org/wiki/Face\\_ID](https://en.wikipedia.org/wiki/Face_ID).



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. Source: [1].

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.

By using the claim that with a biometric system one may ‘... have the same effect as using the same password on many different systems ...’ the authors seem to have neglected the requirement of ISO/IEC 24745 [4]; 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’ [4].

Such systems have been available for more than 10 years now. A significant progress towards BTP in general and renewability specifically was achieved in the European TURBINE project.<sup>35</sup> When the biometric references are created based on a BTP concept, then irreversibility, unlinkability, and renewability of biometric references can be guaranteed.

At the end of the TURBINE project (in the year 2011), the EDPS issued an opinion<sup>36</sup> about BTP 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’.

Furthermore, the concept of BTP has not only been adopted in ISO/IEC 24745, which has reached global attention, but it was also included in the NIST Special Publication 800-63B.<sup>37</sup>

Following the TURBINE project, two further European projects namely FIDELITY<sup>38</sup> and SWAN<sup>39</sup> further developed BTP mechanisms.

A result of that research was the Bloom filter-based approach [19, 20]; which can provide unlinkable, irreversible, and renewable pseudo-identities with no loss of biometric

recognition performance. The formal proof on the security properties was given in the work of Gomez-Barrero [21]. Other BTP methods, for instance homomorphic encryption (HE), which achieve those goals have been developed since.

We, therefore, recommend this statement should be augmented with a reference to ISO/IEC 24745 and to the recent state of the art on BTP.

## 8 | BIOMETRIC INFORMATION CONVERTED TO A HASH IS NOT RECOVERABLE

EDPS-Statement 12:

To add security to the processing of biometric information, it is recommended to remove the biometric pattern from which the hash or biohash has been obtained. However, there are studies showing that the hash could be reversible, that is, it could be possible to obtain the original biometric pattern, especially if the secret of the key used to generate the hash is violated. Source: [1].

The BioHash mechanism is just one example of transforming a biometric template into a protected biometric reference and by no means is representative for the variety of BTP approaches. BioHash may not achieve top performance in terms of privacy protection and security in a benchmark with other BTP technologies [21, 22]. We can agree that some published BTP schemes are of insufficient security and grant no irreversibility.

On the other hand, research has shown that by fulfilling the requirements of ISO/IEC 24745 [4]; secure template protection is possible: More recent approaches, such as the Bloom filter-based method by Rathgeb et al. [20] in its modified version of [23] have been validated to prevent reconstruction of a biometric sample. Furthermore, the enhanced cascaded Bloom filter approach does not allow the recovery of biometric information [23].

More recently, the progress of HE has validated the assumption that comparison of pseudonymous identities is possible in the HE domain as shown by recent work [24–27]. 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.

## 9 | STORED BIOMETRIC INFORMATION DOES NOT ALLOW THE ORIGINAL BIOMETRIC INFORMATION TO BE RECONSTRUCTED FROM WHICH IT HAS BEEN EXTRACTED

EDPS-Statement 13:

<sup>35</sup> <https://cordis.europa.eu/project/id/216339>.

<sup>36</sup> [https://edps.europa.eu/sites/edp/files/publication/11-02-01\\_fp7\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf).

<sup>37</sup> <https://pages.nist.gov/800-63-3/sp800-63b.html>.

<sup>38</sup> <https://cordis.europa.eu/project/rcn/102324/factsheet/en>.

<sup>39</sup> <https://www.ntnu.edu/iik/swan/>.

Stored biometric information (i.e. pattern) allows the original biometric data (e.g. a face) to be partially reconstructed. Such partial reconstruction sometimes has sufficient accuracy for another biometric system to recognise it as the original one. For example, in facial biometric information there are studies that show that it is possible to get from a robot portrait a faithful representation. The accuracy of the reconstruction depends on the amount of biometric information collected. Source: [1].

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 [25]; that fingerprint samples can be reconstructed from minutiae templates [28]; and that face images can be reconstructed from latent neural network representations [29].

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.

## 10 | BIOMETRIC INFORMATION IS NOT INTEROPERABLE

EDPS-Statement 14:

On the contrary, biometric information processing systems are developed according to standards to ensure their interoperability. Systems that work by comparing the result of applying a hash function on biometric patterns can also be made interoperable by the simple method of sharing keys used during the hashing process. Source: [1].

This statement correctly confirms that biometric standards exist. Since the inauguration of international standardisation committee devoted to biometrics (ISO/IEC JTC1 SC37),<sup>40</sup> numerous standards have been developed.

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.

<sup>40</sup><https://committee.iso.org/home/jtc1sc37>.

## 11 | CONCLUSIONS

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. In order to stay compliant with the European data protection principles, in particular those confirmed in the GDPR, Privacy Enhancing Technologies that have been researched, developed, used and are available should be advanced and deployed. As for all technology, biometric technologies should be carefully implemented, tested, and certified. A pro-active and cognizant approach based on the latest research could foster awareness among the citizens and policymakers, as well as contribute to minimising potential negative effects and perceptions of biometric technologies. In order to promote a better understanding of this subject, it is important to clearly distinguish between technical and policy issues. The European Commission is best placed to provide a continuing key role to support research and development, industrial follow ups and the adoption and deployment of international standards as well as its close interaction with all stakeholders through the EAB.

In view of the importance of the topics and challenges covered, the EAB invites EDPS and aepd to work with EAB to create a new joint white paper addressing all the issues raised in this paper.

### ACKNOWLEDGEMENT

None.

### CONFLICT OF INTEREST

None.

### PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

### DATA AVAILABILITY STATEMENT


Not applicable, as no data was used for this position paper.

### ORCID


*Christoph Busch*  <https://orcid.org/0000-0002-9159-2923>

*Adam Czajka*  <https://orcid.org/0000-0003-2379-2533>

*Farzin Deravi*  <https://orcid.org/0000-0003-0885-437X>

*Pawel Drozdowski*  <https://orcid.org/0000-0003-4758-339X>

*Jascha Kolberg*  <https://orcid.org/0000-0002-3128-8049>

*Raghavendra Ramachandra*  <https://orcid.org/0000-0003-0484-3956>

*Christian Rathgeb*  <https://orcid.org/0000-0003-1901-9468>

### REFERENCES

1. DPS & AEPD: 14 Misunderstandings with regard to Biometric Identification and Authentication. [https://edps.europa.eu/sites/edp/files/publication/joint\\_paper\\_14\\_misunderstandings\\_with\\_regard\\_to\\_identification\\_and\\_authentication\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_authentication_en.pdf). (2020) Accessed July 2020

2. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 2382-37, Information technology – Vocabulary – Part 37: Biometrics (2017)
3. Ross, A.: Some research problems in biometrics: the future beckons. In: Proceedings of 12th International Conference on Biometrics (ICB) (2019)
4. ISO/IEC JTC1 SC27 Security techniques, ISO/IEC 24745:2011, Biometric information protection (2011)
5. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 24722, Multimodal and other multibiometric fusion (2015)
6. Jain, A., Prabhakar, S., Pankanti, S.: On the similarity of identical twin fingerprints. *Pattern Recogn.* 35(11), 2653–2663 (2002)
7. U.S. NIST Face Recognition Vendor Test: NIST. <https://pages.nist.gov/frvt/>
8. Zwiesele, A., et al.: Comparative study of biometric identification systems. In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa (2000)
9. Marcel, S., et al.: Handbook of Biometric Anti-spoofing. Springer (2019)
10. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3:2017, Biometric presentation attack detection – Part 1: Framework (2016)
11. Sousedik, C., Busch, C.: Presentation attack detection methods for fingerprint recognition systems: a survey. *J. Biometrics.* 3(4), 219–233 (2014)
12. Raghavendra, R., Busch, C.: Presentation attack detection methods for face recognition system—a comprehensive survey. *ACM Comput. Surv.* 50(1), 1–37 (2017)
13. Czajka, A., Bowyer, K.: Presentation attack detection for Iris recognition: an assessment of the state-of-the-art. *ACM Comput. Surv.* 51(4), 1–35 (2018)
14. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30107-3:2017, Biometric presentation attack detection – Part 3: Testing and Reporting (2017)
15. Biometrics Security iTC: Biometric Protection Profile. <https://biometricitc.github.io/> (2021). Accessed 26 Oct 2021
16. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30137-1:2019, Use of biometrics in video surveillance systems – Part 1: System design and specification (2019)
17. Uhl, A., et al.: Handbook of Vascular Biometrics. Springer (2020)
18. Ross, A., Pasula, R., Hornak, L.: Exploring multispectral iris recognition beyond 900 nm. In: Proceedings of 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS) (2009)
19. Rathgeb, C., Breiting, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive Bloom filters. In: Proceedings of the 6th IAPR International Conference on Biometrics (ICB 2013), Madrid, 4–7 June 2013
20. Rathgeb, C., et al.: On the application of Bloom filters to iris biometrics. *IET J. Biom.* 3(1), 207–218 (2014)
21. Gomez-Barrero, M., et al.: General framework to evaluate unlinkability in biometric template protection systems. *IEEE Trans. Inf. Forensics Secur.* 13(6), 1406–1420 (2018)
22. ISO/IEC JTC1 SC37 Biometrics, ISO/IEC 30136:2018, Performance testing of biometric template protection schemes (2018)
23. Gomez-Barrero, M., et al.: Unlinkable and irreversible biometric template protection based on Bloom filters. *J. Inf. Sci.* 370–371, 18–32 (2016)
24. Boddeti, V.: Secure face matching using fully homomorphic encryption. In: Proceedings BTAS (2018)
25. Gomez-Barrero, M., et al.: Multi-biometric template protection based on homomorphic encryption. *J. Pattern Recognit.* 67, 149–163 (2017)
26. Drozdowski, P., et al.: 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, 18–20 Sept 2019
27. Kolberg, J., et al.: 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, 9–12 Dec 2019
28. Cappelli, R., et al.: Fingerprint image reconstruction from standard templates. *IEEE Trans. Pattern Anal. Mach. Intell.* 29(9), 1489–1503 (2007)
29. Mai, G., et al.: On the reconstruction of face images from deep face templates. *IEEE Trans. Pattern Anal. Mach. Intell.* 41, 1188–1202 (2018)

**How to cite this article:** Busch, C., et al.: A response to the European Data Protection Supervisor ‘Misunderstandings in Biometrics’ by the European Association for Biometrics. *IET Biom.* 11(1), 79–86 (2022). <https://doi.org/10.1049/bme2.12057>