ARTICLE 29 DATA PROTECTION WORKING PARTY

00720/12/EN
WP193

Opinion 3/2012 on developments in biometric technologies

Adopted on 27th April 2012

Executive Summary

Biometric systems are tightly linked to a person because they can use a certain unique property of an individual for identification and/or authentication. While a person's biometric data can be deleted or altered the source from which they have been extracted can in general neither be altered nor deleted.

Biometric data are successfully and efficiently used in scientific research, are a key element of forensic science and a valuable element of access control systems. They can help to raise the security level and make identification and authentication procedures easy, fast and convenient. In the past the use of this technology was expensive and as a result of this economic constraint the impact on individuals' data protection rights was limited. In recent years this has changed dramatically. DNA analysis has become faster and affordable for almost everyone. The technological progress has made storage space and computing power cheaper; this made online picture albums and social networks with billions of photographs possible. Fingerprint readers and video surveillance devices have become an inexpensive gadget. The development of these technologies has contributed to make many operations more convenient, has contributed to solve many crimes and made access control systems more reliable, but it has also introduced new threats to fundamental rights. Genetic discrimination has become a real problem. Identity theft is no longer a theoretical threat.

While other new technologies that target large populations and have recently raised data protection concerns do not necessarily focus on establishing a direct link to a specific individual - or creating this link requires considerable efforts - biometric data, by their very nature, are directly linked to an individual. That is not always an asset but implies several drawbacks. For instance equipping video surveillance systems and smartphones with facial recognition systems based on social network databases could put an end to anonymity and untraced movement of individuals. On the other hand fingerprint readers, vein pattern readers or just a smile into a camera might replace cards, codes, passwords and signatures.

These and other recent developments are addressed in this Opinion to raise awareness among both the people concerned and the legislative bodies. These technical innovations that are very often presented as technologies that only improve the user experience and convenience of applications could lead to a gradual loss of privacy if no adequate safeguards are implemented. Therefore this Opinion identifies technical and organisational measures aiming at mitigating data protection and privacy risks and that can help to prevent negative impacts on European citizens' privacy and their fundamental right to data protection.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION

1. Scope of the Opinion

In the 2003 Working document on biometrics (WP80) the Article 29 working party (Working Party) explored the data protection questions related to the use of upcoming technologies that were able to electronically read and process biometric data. In the years that have passed the use of this technology has been widely deployed in both the public and private sector and a number of new emerging services have developed. Biometric technologies that once needed significant financial or computational resources have become dramatically cheaper and faster. The use of fingerprint readers is now commonplace. For example, some laptops include a fingerprint reader for biometric access control. Advances in DNA analysis mean that results are now available within a few minutes. Some of the newly developed technologies such as vein pattern recognition or facial recognition are already developed to maturity. Their use in various places of our everyday life is just around the corner. Biometric technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition many of them allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through the growing deployment of these technologies. Every individual is likely to be enrolled in one or several biometric systems.

The purpose of this opinion is to provide a revised and updated framework of unified general guidelines and recommendations on the implementation of privacy and data protection principles in biometric applications. This opinion addresses European and national legislative authorities, the biometric systems industry and users of such technologies.

2. Definitions

Biometric technologies are not new and they have already been tackled in different opinions of the Working Party. This section aims to compile the relevant definitions and provide an update whenever it is necessary.

Biometric data: As already noted by the Working Party in Opinion 4/2007 (WP136), biometric data may be defined as:

> *"biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are*

both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."

Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use.

Biometric data can be stored and processed in different forms. Sometimes the biometric information captured from a person is stored and processed in a raw form that allows recognising the source it comes from without special knowledge e.g. the photograph of a face, the photograph of a finger print or a voice recording. Some other times, the captured raw biometric information is processed in a way that only certain characteristics and/or features are extracted and saved as a biometric template.

Source of biometric data: The source of biometric data can vary widely and includes physical, physiological, behavioural or psychological elements of an individual. According to Opinion 4/2007 (WP136):

"the sources of biometric data (e.g. human tissue samples) cannot be considered as biometric data themselves but can be used for the collection of biometric data (through the extraction of information from them)."

As was stated in the WP80, there are two main categories of biometric techniques

- Firstly, there are physical and **physiological**-based techniques which measure the physical and physiological characteristics of a person and include: fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odour detection, voice recognition, DNA pattern analysis and sweat pore analysis, etc.
- Secondly there are **behavioural**-based techniques, which measure the behaviour of a person and include hand-written signature verification, keystroke analysis, gait analysis, way of walking or moving, patterns indicating some subconscious thinking like telling a lie, etc.

An emerging field of **psychological**-based techniques should also be taken into account. It includes measuring of response to concrete situations or specific tests to conform to a psychological profile.

Biometric template: Key features can be extracted from the raw form of biometric data (e.g. facial measurements from an image) and stored for later processing rather than the raw data itself. This forms the biometric template of the data. The definition of the size (the quantity of information) of the template is a crucial issue. On the one hand, the size of the template should be wide enough to manage security (avoiding overlaps between different biometric data, or identity substitutions), on the other hand, the size of the template should not be too large so as to avoid the risks of biometric data reconstruction. The generation of the template should be a one-way process, in that it should not be possible to regenerate the raw biometric data from the template.

Biometric systems: According to WP80 biometric systems are:

> *"applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person. Authentication/verification applications are often used for various tasks in completely different areas, for different purposes and under the responsibility of a wide range of different entities."*

Due to the recent technological developments it is now also possible to use biometric systems for categorisation /segregation purposes.

The risks which are presented by biometric systems derive from the very nature of the biometric data used in the processing. Therefore a more general definition would be a system that extracts and further processes biometric data.

The processing of biometric data within a biometric system typically involves different processes such as enrolment, storage and matching:

- Biometric enrolment: Encompasses all the processes that are carried out within a biometric system in order to extract biometric data from a biometric source and link this data to an individual. The quantity and the quality of data required during enrolment should be sufficient to allow for his/her accurate identification, authentication, categorisation or verification without recording excessive data. The amount of data extracted from a biometric source during the enrolment phase has to be adequate to the purpose of the processing and the level of performance of the biometric system.

The enrolment phase is typically the first contact that an individual would have with a specific biometric system. In most cases enrolment requires the personal involvement of the individual (e.g. in case of fingerprinting) and therefore may provide a suitable opportunity to provide information and fair processing notification. However it is also possible to enrol individuals without their knowledge or consent (e.g. CCTV systems with embedded facial recognition functionality). The accuracy and security of the enrolment process is essential for the performance of the whole system. An individual may be able to re-enrol with a biometric system to update the recorded biometric data.

- Biometric storage: The data obtained during enrolment can be stored locally in the operations centre where the enrolment took place (e.g. in a reader) for later use, or on a device carried by the individual (e.g. on a smart card) or could be sent and stored in a centralised database accessible by one or more biometric systems.

- Biometric matching: It is the process of comparing biometric data/template (captured during enrolment) to the biometric data/template collected from a new sample for the purpose of identification, verification/authentication or categorisation.

Biometric identification: The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

Biometric verification/authentication: The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one-to-one matching process).

Biometric categorisation/segregation: The categorisation/segregation of an individual by a biometric system is typically the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, it is not important to identify or verify the individual but to assign him/her automatically to a certain category. For instance an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.

Multi-modal biometrics: They can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system (it is also called multi-level biometrics). Biometric systems use two or more biometric traits / modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric. Some studies include within this category also systems working by performing multiple readings of the same biometric or those using multiple algorithms for feature extraction on the same biometric sample. Examples of multimodal biometric systems are the ePassport at EU level as well as the US-VISIT Biometric Identification Services in the United States.

Accuracy: When biometric systems are used it is difficult to produce 100% error-free results. This may be due to differences in the environment at data acquisition (lighting, temperature, etc.) and differences in the equipment used (cameras, scanning devices, etc.). The most used conventional performance evaluation metrics are the False Accept Rate and the False Reject Rate and they can be adjusted to the system is use:

- The False Accept Rate (FAR): It is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. It measures the percentage of invalid inputs which are incorrectly accepted. It is also known as the false positive rate.

- The False Reject Rate (FRR): It is the probability that the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. It is also known as the false negative rate.

With proper system tuning and setup adjustment, critical errors of biometric systems can be minimised to the level allowed for the operational use by reducing the risks of incorrect assessments. A perfect system will have a zero FAR and FRR but, more commonly, they are negatively correlated. The increase of the FAR often reduces the level of the FRR.

It is important to evaluate the purpose of processing, both the FAR and FRR and the population size when assessing whether or not the accuracy of a particular biometric system is acceptable. Furthermore assessing the accuracy of a biometric system may also take into account the ability to detect a live sample. For example, latent fingerprints can be copied and used to create false fingers. A fingerprint reader must not be fooled into making a positive identification in such a situation.

3. Legal analysis

The relevant legal framework is the Data Protection Directive (95/46/EC). The Working Party already stated in WP80 that biometric data are in most cases personal data. Therefore they may only be processed if there is a legal basis and the processing is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Purpose

A prerequisite to using biometrics is a clear definition of the purpose for which the biometric data are collected and processed, taking into account the risks for the protection of fundamental rights and freedoms of individuals.

Biometric data can for example be collected to ensure or increase the security of processing systems by implementing appropriate measures to protect personal data against unauthorised access. In principle, there are no obstacles to the implementation of appropriate security measures based on biometric features of the persons in charge of the processing in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. However it should be kept in mind that the use of biometrics per se does not ensure enhanced security, because many biometric data can be collected without the knowledge of the concerned person. The higher the envisaged security level is the less biometric data alone will be able to come up with that aim.

The principle of purpose limitation has to be respected together with the other data protection principles; especially the proportionality, necessity and data minimisation principles have to be kept in mind when the different purposes of an application are defined. Whenever it is possible, the data subject must have the choice between the several purposes of an application with multiple functionalities, in particular if one or several of them requires the processing of biometric data.

Example:
The use of electronic devices providing specific authentication procedures based on biometric data has been recommended in connection with the security measures to be taken in case of:

- processing of personal data collected by telephone operators during wiretapping activities authorised by a court;
- both access to traffic data (and location data) retained for justice purposes by the providers of publicly available electronic communications services or of a public communications network and access to relevant premises in which those data are processed;
- collection and storage of genetic data and biological samples.

Photographs on the internet, in social media, in online photo management or sharing applications may not be further processed in order to extract biometric templates or enrol them into a biometric system to recognise the persons on the pictures automatically (facial recognition) without a specific legal basis (e.g. consent) for this new purpose. If there is a legal basis for this secondary purpose the processing must also be adequate, relevant and not excessive in relation to that purpose. If a data subject has consented that photographs where he appears may be processed to automatically tag him in an online photo album with a facial recognition algorithm, this processing has to be achieved in a data protection friendly way: biometric data not needed anymore after the tagging of the images with the name, nickname or any other text specified by the data subject must be deleted. The creation of a permanent biometric database is a priori not necessary for this purpose.

Proportionality

The use of biometrics raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. As biometric data may only be used if adequate, relevant and not excessive, it implies a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way.

In analysing the proportionality of a proposed biometric system a prior consideration is whether the system is necessary to meet the identified need, i.e. is essential for satisfying that need rather than being the most convenient or cost effective. A second factor to take into consideration is whether the system is likely to be effective in meeting that need by having regard to the specific characteristics of the biometric technology planned to be used[1]. A third aspect to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate. The fourth aspect in assessing the adequacy of a biometric system is to consider whether a less privacy intrusive means could achieve the desired end[2].

Example:
In a health & fitness club, a centralised biometric system based on the collection of fingerprints is installed in order to grant access to the gym premises and to the related services only to the customers that have paid their fees.
To run such a system the storage of fingerprints of all customers and staff members would be required. This biometric application seems to be disproportionate in relation to the need of controlling access to the club and facilitating the management of subscriptions. Other measures such as a simple checklist or the use of RFID tags or a swipe card that do not require the processing of biometric data can easily be imagined to be equally practicable and effective.

The Working Party warns of the risks involved in the use of biometric data for identification purposes in large centralised databases, given the potentially harmful consequences for the persons concerned.

The major impact on the human dignity of data subjects and the fundamental rights implications of such systems should be taken into account. In the light of the European Convention for the Protection of Human Rights and Fundamental Freedoms and of the case law of the European Court on Human Rights on Article 8 of the Convention, the Working Party emphasizes that any interference with the right to data protection is only to be allowed

[1] Biometrics will be used for either verification or identification purposes: a biometric identifier could be judged technically suitable for the one and not for the other (for example technologies characterised by low failed rejection rates should be preferred in systems designed to be used for identification purposes in law enforcement).

[2] For example, smart cards or other methods that do not collect or centralize biometric information for authentication purposes.

on condition that it is in accordance with the law and that it is necessary, in a democratic society, to protect an important public interest[3].

To ensure respect for these conditions, it is necessary to specify the aim that is pursued by the system and to assess proportionality of the data to be entered in the system as related to the said aim.

To that end, the controller has to establish whether the processing and its mechanisms, the categories of the data to be collected and processed and the transfer of information contained in the database are necessary and indispensable. The adopted security measures must be adequate and effective. The controller has to consider the rights to be granted to the individuals the personal data refer to, and ensure that a proper mechanism to exercise such rights is incorporated in the application.

Example:
Use of biometric data for identification purposes. Systems analysing the face of a person as well as systems that analyse the DNA of a person can contribute very efficiently to the fight against crimes and efficiently reveal the identity of an unknown person suspected of a serious crime. These systems used however on a large scale produce serious side effects. In the case of facial recognition where biometric data can be easily captured without the knowledge of the data subject a widespread use would terminate anonymity in public spaces and allow consistent tracking of individuals. In the case of DNA data the use of the technology comes with the risk that sensitive data about the health of a person could be revealed.

Accurate

Biometric data processed must be accurate and relevant in proportion to the purpose for which there they were collected. The data must be accurate at enrolment and when establishing the link between the person and the biometric data. Accuracy at enrolment is also relevant to the prevention of identity fraud.

Biometric data are unique and most of them generate a unique template or image. If used widely, in particular for a substantial proportion of a population, biometric data may be considered as an identifier of general application within the meaning of Directive 95/46/EC. Article 8, §7 of Directive 95/46/EC would then be applicable and Member States would have to determine the conditions of their processing.

[3] See European Court of Justice, Judgment of 20 May 2003 joined cases C-465/00, C-138/01 and C-139/01 (Rechnungshof vs. Österreichischer Rundfunk and Others), European Court of Human Rights, Judgment of 4 December 2008, Application nos. 30562/04 and 30566/04 (S. and Marper vs. the United Kingdom) and Judgment of 19 July 2011, Application nos. 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 and 64027/09 (Goggins and others vs. the United Kingdom).

Data minimisation

A specific difficulty may arise as biometric data often contain more information than necessary for matching functions. The principle of data minimisation has to be enforced by the data controller. Firstly, this means that only the required information and not all available information should be processed, transmitted or stored. Second, the data controller should ensure that the default configuration promotes data protection, without having to enforce it.

Retention period

The controller should determine a retention period for biometric data that should not be longer than is necessary for the purposes for which the data were collected or for which they are further processed. The controller must ensure that the data, or profiles derived from such data, are permanently deleted after that justified period of time.

The difference must be clear between general personal data that may be needed for a longer period of time and biometric data that are of no use anymore, e.g. when the data subject is no longer granted access to a specific area.

Example:
An employer operates a biometric system to control the access to a restricted area. An employee's role no longer requires him/her to access the restricted area (e.g. changes responsibility or job). In this case, his biometric data must be deleted since the purpose for which they were collected no longer applies.

3.1. Legitimate ground

The processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of Directive 95/46/EC.

3.1.1. Consent, Article 7(a)

The first such ground of legitimacy given in Article 7(a) is where the data subject has given consent to the processing. According to the data protection directive, Article 2(h), consent must be freely given, specific and informed indication of the data subject's wishes. It must be clear that such consent cannot be obtained freely through mandatory acceptance of general terms and conditions, or through opt-out possibilities. Furthermore, consent must be revocable. In this regard, in its opinion on the definition of consent, the Working Party underlines various important aspects of the notion: the validity of consent; the right of individuals to withdraw their consent; consent given before the beginning of the processing; requirements regarding the quality and the accessibility of the information[4].

In many cases in which biometric data are processed, without a valid alternative like a password or a swipe card, the consent could not be considered as freely given. For instance, a system that would discourage data subjects from using it (e.g. too much time wasted for the user or too complicated) could not be considered as a valid alternative and then would not lead to a valid consent.

[4] WP 187, Opinion 15/2011 on the definition of consent.

Examples:
In the absence of other alternative legitimate grounds, a biometric authentication system could be used to control access to a video club only if the customers are free to decide whether to avail themselves of the said system. This means that alternative, less privacy-intrusive mechanisms must be made available by the movie club owner. Such a system will permit a customer who is unwilling or unable to undergo fingerprinting because of his/her personal circumstances to dissent. The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as legitimate ground.

In a kindergarten a vein pattern scanner is installed to check every adult person entering (parents and members of staff) whether they are entitled to enter or not. To run such a system the storage of fingerprints of all parents and staff members would be required. Consent would be a questionable legal basis especially for the employees as they might not have a real choice to refuse the use of such a system. It would be questionable for the parents too as long as there is no alternative method to enter the kindergarten.

Although there may be a strong presumption that consent is weak because of the typical imbalance between employer and employee, the Working Party does not rule it out completely "*provided there are sufficient guarantees that consent is really free*"[5].

Therefore consent in the employment context has to be questioned and duly justified. Instead of seeking consent, employers could investigate whether it is demonstrably necessary to use biometrics of employees for a legitimate purpose and weigh that necessity against the fundamental rights and freedoms of the employees. In cases where the necessity can be adequately justified, the legal basis of such a processing could be based on the legitimate interest of the controller as defined in Article 7(f) of the Directive 95/46/EC. The employer must always seek the least intrusive means by choosing a non-biometric process, if possible.

However, as described in 3.1.3, there may be cases where a biometric system may be in the legitimate interest of the data controller. In these cases consent would not be required.

Consent is only valid when sufficient information on the use of biometric data is given. Since biometric data may be used as a unique and universal identifier providing clear and easily accessible information on how the specific data are used is to be regarded as absolutely necessary to guarantee fair processing. Therefore this is a crucial requirement for a valid consent in the use of biometric data.

Examples:
A valid consent to an access control system that uses fingerprints requires information whether the biometric system creates a template that is unique to that system or not. If an algorithm is used that creates the same biometric template in different biometric systems the data subject needs to know that he might be recognised in several different biometric systems.

Someone uploads his picture in a photo album on the internet. Enrolling this picture into a biometric system requires an explicit consent based on exhaustive information on what is done with the biometric data, how long and for which purposes they are processed.

[5] WP 187, Opinion 15/2011 on the definition of consent.

As consent can be revoked at any time data controllers need to implement technical means that can reverse the use of biometric data in their systems. A biometric system operating on the basis of consent needs therefore to be able to efficiently remove all identity links it created.

3.1.2. Contract, Article 7(b)

Processing of biometric data can be necessary for the performance of a contract to which the data subject is party or can be necessary in order to take steps at the request of the data subject prior to entering into a contract. It has however to be noted that this applies in general only when pure biometric services are provided. This legal basis cannot be used to legitimate a secondary service that consists in enrolling a person into a biometric system. If such a service can be separated from the main service the contract for the main service cannot legitimate the processing of biometric data. Personal data are not goods that can be asked for in exchange of a service, therefore contracts that foresee that or contracts that offer a service only under the condition that someone consents to the processing of his biometric data for another service cannot serve as legal basis for that processing.

Examples:
a) Two brothers submit hair samples to a laboratory to perform a DNA test to find out if they truly are brothers. The contract with the laboratory to perform this test is a sufficiently legal basis for the enrolment and the processing of biometric data.

b) Someone submits a photo to show to his friends in his photo album in a social network. If the contract (terms of service) provides that the use of the service is bound to the enrolment of this user in a biometric system, this provision is not a sufficient legal basis for this enrolment.

3.1.3. Legal obligation, Article 7(c)

Another legal ground for processing personal data is if the processing is necessary for compliance with a legal obligation to which the controller is subject. That is for example the case in some countries when passports[6] and visas[7] are issued and/or used.

3.1.4. Legitimate interests of the data controller, Article 7(f)

According to Article 7 of Directive 95/46/EC, the processing of biometric personal data can also be justified if it is "necessary for the purposes of the legitimate interests pursued by the

[6] Fingerprints have been integrated in passports in compliance with the EU Council Regulation 2252/2004 of 13 December 2004 and in resident permits in compliance with EU Council Regulation 1030/2002 of 13 June 2002.

[7] Registration of biometric identifiers in the Visa Information System (VIS) is established by Regulation (EC) No 767/2008 l of 9 July 2008 concerning Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). See also Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006)269 final). WP134; Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final) WP 110; Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS) WP 96.

controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

That means that there are cases where the use of biometric systems is in the legitimate interest of the data controller. Such an interest is however only legitimate when the controller can demonstrate that his interest objectively prevails over the data subjects' right not to be enrolled in a biometric system. For example when the security of high risk areas needs to be specifically ensured by a mechanism that can precisely verify if the persons are entitled to access these areas, the use of a biometric system can be in the legitimate interest of the controller. In the example below of a biometric access control system to a laboratory the controller cannot offer the employee an alternative mechanism without directly impacting on the security of the restricted area as there are no alternative less invasive measures suitable for achieving an adequate level of security for this area. Therefore it is in his legitimate interest to implement the system and enrol a limited number of staff. He does not need to obtain their consent. However, in the case in which a legitimate interest of the controller is a valid legal ground for the processing, as always, all other data protection principles still apply, notably the principles of proportionality and data minimisation.

Example:
In a company doing research on dangerous viruses a laboratory is secured by doors that open only after a successful fingerprint and iris scan verification. This is implemented to make sure that only the persons familiar with the specific risks, trained on the procedures and found trustworthy by the company can experiment with these dangerous materials. The legitimate interest of the company to make sure that only the relevant persons may enter a restricted area to guarantee that the security risks coming with the access of that specific area can be reduced significantly overrides the wish of the persons that their biometric data is not processed.

As a general rule, the use of biometrics for general security requirements of property and individuals cannot be regarded as legitimate interest overriding the interests or fundamental rights and freedoms of the data subject. On the contrary, the processing of biometric data can only be justified as a required tool securing the property and/or individuals, where there is evidence, on the basis of objective and documented circumstances, of the concrete existence of a considerable risk. To that end the controller needs to prove that specific circumstances pose a concrete, considerable risk, which the controller is required to assess with special care. In order to comply with the proportionality principle, the controller, in presence of these high risk situations, is obliged to verify if possible alternative measures could be equally effective but less intrusive in relation to the aims pursued and choose such alternatives.
The existence of the circumstances in question should also be reviewed on a regular basis. Based on the outcome of this review, any data processing operation that is found not to be justified any longer must be terminated or suspended.

3.2. Data controller and Data processor

Directive 95/46/EC places obligations on the data controllers with regard to their processing of personal data. In the context of biometrics different types of entities can be data controller, for example employers, law enforcement or migration authorities.

The Working Party recalls the guidance provided in its Opinion on the concepts of controller and processor[8], which contains effective clarifications on how to interpret these core definitions of the Directive.

3.3. Automated processing (Art 15 Directive)

When systems that are based on the processing of biometric data are used, careful attention should be paid to the potential discriminatory consequences for the persons rejected by the system. Furthermore, in order to protect the individual's right not to be subject to a measure affecting him based solely on automated processing of data, appropriate safeguards must be introduced such as human interventions, remedies or mechanisms allowing the data subject to put (forward) his point of view.

According to Article 15 of Directive 95/46/EC *"Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct etc."*

3.4. Transparency and information of the data subject

According to the principle of fair processing, data subjects must be aware of the collection and/or use of their biometric data (Art. 6 of Directive 95/46/EC). Any system that would collect such data without the data subjects' knowledge must be avoided.

The data controller must make sure that data subjects are adequately informed about the key elements of the processing in conformity with Article 10 of the data protection directive, such as their identity as controller, the purposes of the processing, the type of data, the duration of the processing, the rights of data subjects to access, rectify or cancel their data and the right to withdraw consent and information about the recipients or categories of recipients to whom the data are disclosed. As the controller of a biometrics system is obliged to inform the data subject, biometrics must not be taken from somebody without his knowledge.

3.5. Right to access biometric data

Data subjects have a right to obtain from the data controllers access to their data, in general including their biometric data. Data subjects also have a right to access possible profiles based on these biometric data. If the data controller has to ascertain the identity of the data subjects to grant this access, it is essential that such access is provided without processing additional personal data.

3.6. Data security

The data controllers must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.[9]

Any data collected and stored must be appropriately secured. Designers of systems must engage with appropriate security experts to ensure that security vulnerabilities are appropriately tackled, especially if existing systems are migrated to the internet.

---

[8] WP169, Opinion 1/2010 on the concepts of "controller" and "processor".

[9] Article 17 (1) of Directive 95/46/EC.

3.7. Safeguards for people with special needs

The use of biometrics could impact significantly on the dignity, privacy and the right to data protection of vulnerable people such as young children, elderly people and persons physically unable to complete the enrolment process successfully. Given the potentially harmful consequences for the persons concerned, more stringent requirements will have to be met in the impact assessment process of any measure interfering with an individual's dignity in terms of questioning the necessity and proportionality as well as the possibilities of the individual to exercise his right to data protection in order for that measure to be deemed admissible. Appropriate safeguards must be in place against the risks of stigmatization or discrimination of those individuals either because of their age or because of their inability to enrol.

Regarding the introduction of a generalized legal obligation of collecting biometric identifiers for these groups, notably, for young children and elderly people at border controls for identification purposes, the Working Party has taken the view that – "*for the sake of the person's dignity and to ensure reliability of the procedure – the collection and processing of fingerprints should be restricted for children and for elderly people and that the age limit should be consistent with the age limits in place for other large EU biometric databases (Eurodac, in particular*)."[10]

In any case, specific safeguards (such as appropriate fall-back procedures) should be implemented so as to ensure the respect for human dignity and fundamental freedoms of any individual that is unable to complete the enrolment process successfully and thereby avoid burdening such individual with the imperfections of the technical system [11].

3.8. Sensitive data

Some biometric data could be considered sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health. For example DNA data of a person often include health data or can reveal the racial or ethnic origin. In this case DNA data are sensitive data and the special safeguards provided by article 8 must apply in addition to the general data protection principles of the Directive. In order to assess the sensitivity of data processed by a biometric system the context of the processing should also be taken into account[12].

3.9. Role of national DPAs

Taking into consideration the growing standardisation of biometric technologies for interoperability, it is generally accepted that the centralised storage of biometric data increases both the risk of the use of biometric data as a key to interconnect multiple databases (which might lead to creating detailed profiles of an individual) and the specific dangers of the reuse of such data for incompatible purposes especially in the case of unauthorised access.

---

[10] WP134 - Opinion N° 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006)269 final).

[11] Cf. WP134 - Opinion N° 3/2007, p. 8.

[12] Cf. WP 29 Advice paper on special categories of data ("sensitive data") Ref. Ares (2011)444105 - 20/04/2011.

The Working Party recommends that systems that use biometric data as a key to interconnect multiple databases require additional safeguards, as this kind of processing is likely to present specific risks to the rights and freedoms of data subjects (Article 20 of Directive 95/46/EC). In order to ensure suitable safeguards and in particular to mitigate the risks for data subjects, a controller should consult the competent national data protection authority before such measures are introduced.

4. New developments & technological trends, new scenarios

4.1. Introduction

Biometric technologies have been used for a long time mainly by Governmental authorities, but recently the situation has gradually shifted to one where commercial organisations play a primary role using these technologies and developing new products.

One of the key drivers of that situation is that the technology has matured in such a way that biometric systems that only worked well under controlled conditions have been refined and are now suitable for extensive use in a range of different environments. In that sense, biometrics are, in some cases, replacing or enhancing conventional identification methods, particularly those based on multiple identification factors needed for strong authentication systems. Biometric technologies are also increasingly being used in applications that can quickly and conveniently identify someone at the price of a lower accuracy level.

The use of biometric technologies is also gradually spreading from their original sphere of application: identification and authentication to behaviour analysis, surveillance and fraud prevention.

Advances in computer technologies and networks are also leading to the rise of what is considered the second generation of biometrics based on the use of behavioural and psychological traits alone or combined with other classical systems forming multimodal systems. To complete the picture, there is a gradual move to the use of biometrics in ambient intelligence and ubiquitous computing developments.

4.2. New trends on biometrics

There are a number of biometric technologies that can be considered mature technologies with several applications in law enforcement, e-government and commercial systems. A non-exhaustive list would cover fingerprints, hand geometry, iris scan and some types of facial recognition. There are also some body trait analysis biometric technologies that are emerging. While some of them are new, some traditional biometric technologies, are taking new impulse from new processing capacities.

Typical elements of these new systems are the use of body traits allowing the categorisation / identification of individuals and the remote collection of such traits. The collected data are used for profiling, remote surveillance or even more complex tasks like ambient intelligence.

This became possible because of the continuous development on sensors allowing the collection of new physiological characteristics as well as new ways to process traditional biometrics.

Mention should also be made to the use of the so-called soft biometrics, defined by the use of very common traits not suitable to clearly distinguish or identify an individual but that allow enhancing the performance of other identification systems.

Another essential element of the new biometric systems is the potential to collect information from a distance or in motion without the need of cooperation or action required from the individual. Even though it is still not a fully developed technology, a huge effort is being made particularly for law enforcement purposes.

What is rapidly progressing is the use of multimodal systems using different biometrics in a simultaneous way or multiple readings/units of the same biometrics that can be adjusted in order to optimize the trade of security / convenience of the biometric systems. This can reduce the false acceptance rate, improve the results of a recognition system or can facilitate the collection of data of a larger population by balancing the non-universality of one source of biometric data by combining it with another.

Biometric systems are increasingly used by both public and private entities; traditionally in the public sector law enforcement uses biometric data regularly; in the financial, banking and e-health sector the use of biometrics is rapidly growing as well as in other sectors like education, retail and telecommunication. This development will be fuelled by the new features derived from the convergence / fusion of existing technologies. An example is the use of CCTV systems allowing both the collection and analysis of biometrics and human behaviour signatures.

The above can be also seen as a change in the focus on development in biometric systems from identifying tools to soft recognition purposes, in other words, from identification to detection of behaviour or specific needs of people. This also open doors to uses far different from large scale security applications: personal security, gaming and retail will benefit from an enhanced man-machine interaction allowing more than identification, or categorisation of an individual.

4.3. Impact on privacy and data protection

Since the very beginning of their implementation, biometric systems have been acknowledged to have the potential to raise strong concerns on several fields, including privacy and data protection, which have certainly influenced their social acceptance and fuelled the debate over the legality and limits of their use and the safeguards and guarantees needed to mitigate the identified risks.

Classical reluctance to biometric systems has been linked to the protection of individual rights, and still is. Nevertheless, new systems and developments to existing systems raise a range of concerns. This includes the possibility of covert collection, storage and processing as well as the collection of material with highly sensitive information that can invade the most intimate space of the individual.

Function creep has been a serious concern since the biometric technologies and systems were first used; even though that is a well-known and addressed risk in traditional biometrics, it is undoubtedly clear that the higher technical potential of new computer systems raises the risk of data being used against their original purpose.

Covert techniques allow for the identification of individuals without their knowledge, resulting in a serious threat for privacy and a leak of control over personal data. That has serious consequences on their capacity to exercise free consent or simply get information about the processing. Moreover some systems can secretly collect information related to emotional states or body characteristics and reveal health information resulting in a non-proportional data processing as well as in the processing of sensitive data in the meaning of article 8 of the Directive 95/46/EC.

Taking into account the fact that biometric technologies cannot ensure full accuracy, there is always an implicit risk coming from incorrect identifications. Such false positives result in decisions affecting individual rights. Identity theft based on the use of spoofed or stolen biometric sources can lead to serious damages. Unlike in other identification systems, the individual cannot be simply provided with a new identification just because it is compromised.

Reference should be made to profiling in the context of taking automated decisions or to predict behaviour or preferences in a specific situation. Some biometric data can reveal physical information about an individual. This can be used for targeting and profiling purposes but also end up in discrimination, stigmatization or unwanted confrontation with non-expected / desired information.

4.4. Reference to specific biometric systems and technologies

4.4.1. Vein pattern & combined uses

Two main technologies in use are based on vein pattern recognition: palm vein recognition and finger vein recognition, both techniques are now widely used, particularly in Japan.

Technically, vein pattern recognition relies on the template of the veins captured by an infrared camera when the finger or the hand is enlightened by near infrared light. The image acquired is processed to outline the characteristics of the vein pattern resulting in a post-processed image of the vascular network. The main advantage of such technology is the fact that each individual does not leave a trace of their biometric feature[13] as there is no requirement to "touch" the reader. As of today it is also difficult to collect the biometric data without the consent of the data subject. Finally, this technique can also be used to detect if the subject presented to the system is alive or not by analysing if the blood is flowing.

Vein pattern recognition can be used for logical access applications and physical access to premises. The manufacturers also offer the ability to include the sensor in other products, especially for banking purposes.

Data protection risks associated with the use of vein pattern systems can be described as follows:

- Accuracy: the performance level of vein pattern is high, as this technology is seen as a viable alternative to fingerprints. Vein recognition offers also a low "Failure to Enrol Rate" (FER), as it is not subject to the deteriorations of the finger or the hand. These technologies still have not been experimented/used with very large population register (in Japan, the template is compared with the template stored in the smart card). In some cases, this technology may also be affected by climatic conditions that influence the vascular system (heat, pressure, etc.).
- Impact: the impact of vein pattern systems on data protection is limited, as the biometric data is not easily collected and the use of vein pattern is today limited to applications of the private sector.

[13] Some authors claim that technologies associated to vein recognition can reveal diseases like hypertension or vascular abnormalities.

- Consent & Transparency: as vein pattern data can be collected only with the use of near-infrared lighting and cameras, it can be considered that the person is aware of the processing and gives its consent by applying its finger or hand to the reader. However, likewise any biometric system, this presumption should be mitigated in some specific contexts, for instance when the person is an employee of the data controller.

- Further purpose or purposes of processing: as of today, vein pattern data presents limited risks regarding its use for further purpose. This risk may increase if this kind of processing is generalised and if spoofing is made easier.

- Linkability: vein pattern data does not provide information that can be linked with other data, except vein pattern data from another processing.

- Tracking / Profiling: the risk of tracking/profiling with vein pattern data is limited, as long as this type of biometrics is not widely used, for instance in a central database for payment cards.

- Processing of sensitive data: the only sensitive data that could be derived from vein pattern data concerns health condition but no formal evaluation has been conducted on this topic so far.

- Revocability: vein pattern data seems very stable with time but this assertion must be confirmed experimentally (vein pattern systems are too recent to provide confirmed results). Vein pattern data should therefore be considered irrevocable.

- Anti-spoofing protection: vein pattern data spoofing has not been extensively explored yet but a recent research showed that it is possible to spoof a palm vein reader[14]. The main difficulty for spoofing vein pattern data is to collect a sample of the biometric data.

4.4.2. Fingerprints & combined uses

Fingerprint recognition is among the oldest and most widely studied and most extensively deployed biometric systems. Identification by fingerprints has been used for more than 100 years in law enforcement for both verification and identification tasks. It is founded in the fact that every individual has unique fingerprints showing specific characteristics that can be measured in order to decide if a fingerprint matches against an enrolled sample.

Enrolment requires the individual to be physically present as well as, depending on the expected use, well trained personnel in order to ensure good data quality. Fingerprint capture is not a trivial task. In that sense matching accuracy will depend on the image quality in relation to the image technique. Techniques may vary from one or two fingers to all ten fingers taken on flat or rolled mode. Depending of the system, fingerprints can be used just for verification (1:1) or for identification and matching with traces (1: n). However, as some studies have shown, a fraction of the population is not able to enrol for different reasons, posing a problem that claims for the existence of appropriate fall-back procedures, particularly for large systems, in order to avoid depriving individuals of something they are entitled.

[14] See: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

Even not being in principle a highly invasive method, it can be felt as such because it comes with the negative image of being treated as a suspect due to its common use in law enforcement.

Fingerprints show different features than can be used for verification / identification purposes although minutiae analysis is still the most used technique. The development of new techniques (i.e. high resolution scanners) will allow the use of other features. Techniques have further developed also with regard to the identification capabilities allowing the use of large databases for identification purposes.

In that sense, the most advanced systems are the so called automated fingerprint identification systems (AFIS) used for law enforcement purposes that can be used to exchange data respectively by searching in different repositories in cross border locations. The exchange of data faces problems related to different locations, formats and levels of quality.

Examples of AFIS at EU level are Eurodac and the Visa Information System that - according to the expectations - will be among the largest databases in the world considering that approximately 70 million fingerprints will be stored in those systems. In its previous opinions the Working Party raised several questions on the use of large scale databases considering the need to ensure proportionality. Especially reliability problems in terms of false-positive and false-negative findings, effective access control to these databases and problems related to the use of fingerprints of children and elderly people need to be addressed.

Templates are commonly used in biometric systems based on fingerprinting and are usually considered by system providers as a way to protect the individual. Nevertheless, depending on the system / algorithm used to generate the template, there are potential risks related to the possibility to link templates with other fingerprint databases in order to identify individuals.

The use of systems to circumvent fingerprint recognition systems by using artificial fingers or fingerprints made from artificial material allowing identity theft practices is also a relevant issue. There are different approaches to reduce the vulnerability of these systems such as live detection, systems based on the recognition of multiple fingers and also the use of adequate human supervision for enrolment and identifications / verification tasks.

There are data protection concerns associated with the use of fingerprints that can be briefly described as follows:

- Accuracy: Even though fingerprints eventually present a high accuracy rate, this can be challenged due to limitations related to the information -low quality of the data or non-consistent acquisition process – or representation - features selected or quality of the extraction algorithms –issues. This can lead to false rejection or false matches.

- Impact: The irreversibility of the process can reduce the possibility of the individual of exercising their rights or to reverse decisions adopted based on a false identification. The reliance on the accuracy of fingerprinting can make possible mistakes harder to rectify, leading to far reaching consequences for individuals. This needs to be taken into account when the proportionality of the processing in relation to the specific decision to be taken based on the fingerprints is assessed. It should be also mentioned that lack of security measures can lead to identity theft that can have a strong impact for the individual.

- Linkability: fingerprints provide potential for misuse as the data can be linked with other databases. This possibility of linking up to other databases can lead to uses non-

compatible with the original purposes. There are some techniques, like convertible biometrics or biometric encryption that can be used to reduce the risk.

- Processing of sensitive data: According to some studies, fingerprint images can reveal ethnical information of the individual[15].

- Further purposes or purposes of processing: Central storage of data, especially on large databases, implies risks associated with data security, linkability and function creep. This allows, in absence of safeguards, the use of the fingerprints for purposes different than those that initially justified the processing.

- Consent & Transparency: Consent is a core issue in the use of fingerprints for uses other than in law enforcement. Fingerprints can be easily copied from latent prints and even photographs without the individual's knowledge. Other issues concerning consent are those related to obtaining child's consent and the role played by parents in this regard (e.g. for fingerprinting in schools) as well as the validity of consent for providing fingerprints in a labour context.

- Revocability: fingerprint data are very stable with time and should be considered irrevocable. A fingerprint template may be revoked under certain conditions.

- Anti-spoofing protection: fingerprints can be easily collected because of the multiple tracks of fingerprints an individual leaves behind. Moreover, false fingerprints can be used with many systems and sensors, especially when such systems do not include specific anti-spoofing protection. The success of an attack depends largely on the type of sensor (optical, capacitive, etc.) and the material used by the attacker.

Example:
A hospital uses fingerprints in a central database to authenticate patients in a radiotherapy service to make sure the correct treatment is delivered to the correct patient. Fingerprints are preferred to vein pattern because the treatment impairs the vascular system. Moreover, a central database is used because patients' condition (age, pathology) implies high risk of lost badges that would block the access to the treatment. In this case, the use of fingerprints appears to be an appropriate solution.

4.4.3. Facial recognition & combined uses

The face, like fingerprints, has been used extensively as a source of biometric data for a number of years. More recently it is not only identity that can be determined from a face but physiological and psychological characteristics such as ethnic origin, emotion and wellbeing. The ability to extract this volume of data from an image and the fact that a photograph can be taken from some distance without the knowledge of the data subject demonstrates the level of data protection issues which can arise from such technologies.

Facial recognition as a means for identification and verification has not gone unnoticed by law enforcement, other public authorities or indeed private organisations. For many years photographs have appeared on passports, driving licences, national identity cards and mug shots. It is not uncommon to have a photograph printed on an access control or other

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm and http://www.crime-scene-investigator.net/fingerprintpatterns.html

organisation identity card. These images have typically been taken under controlled lighting and limited to a front or profile view of the individual. Using such a controlled set of images was a natural place to start the automatic processing and recognition of individuals. This ability has since been surpassed and the technology is at the point where identification is possible from images using a range of cameras, viewpoints and lighting conditions. There is also a huge volume of images publically available on the internet, such as those uploaded to social networks and other publically available galleries. Such risks are not confined to traditional images as facial recognition has been successfully integrated into real-time video feeds. By adding new processing capabilities into an existing system (e.g. facial recognition into CCTV) data controllers must recognise that this may change the specified purpose or purposes of the original system and re-assess the privacy impact of the change.

Data protection risks associated with the use of facial recognition systems can be described as follows:

- Accuracy: If the quality of images cannot be guaranteed there is a risk that the accuracy will be compromised. If a face is not captured (obscured by hair or a hat) it is clear that a matching or categorisation cannot take place without a high degree of error. Pose and illumination variations remain a big challenge for facial recognition, highly affecting the accuracy.

- Impact: The specific impact on data protection of a particular facial recognition system will depend on its purpose and particular circumstance. A categorisation system to count demographics of visitors to an attraction with no recording capabilities will have a different impact on data protection to that from a system used for covert surveillance by law enforcement to identify potential troublemakers.

- Consent & Transparency: A data protection risk not seen in many other types of biometric data processing is the fact that images can be captured and processed from a range of viewpoints, environmental conditions and without the knowledge of the data subject. In Opinion 15/2011 on the definition of consent the Working Party highlights the fact that in order for consent to be a legal basis for processing it must be "informed". If the data subject has no knowledge of the processing of images for the purposes of facial recognition this cannot be the case. Even if the data subject is aware that a camera is operating there may be no visual clues to differentiate between a live or recording CCTV system and a lens capturing images for a facial recognition system.

- Further purpose or purposes of processing: Once captured, whether legitimately or unlawfully, digital images can be easily shared or copied for processing in different systems from those which they were originally intended. This is evident in the realm of social media where users upload their personal photographs to share with their family, friends and colleagues. Once within the social media platform images are available for re-use by the platform itself for a range of purposes some of which may be introduced into the platform sometime after the image was captured and/or uploaded.

- Linkability: A large number of online services allow users to upload an image to link with the user's profile. Facial recognition can be used to link across the profiles of different online services (through the profile picture) but also between the online and offline world. It is not out-with the realms of possibility to take a photograph of a

person in the street and in real time determine their identity by searching through these public profile pictures. Third party services can also trawl through profile photographs and others which are publically available to create huge collections of images in order to associate a real world identity with such images.

- Tracking / Profiling: An identification system could also be used if there is no knowledge of the real-world identity of an individual. A facial recognition system within a shopping centre or similar public area could be used to track routes and habits of individual shoppers. Purposes could be for effective queue management or product placement in order to improve the customer experience. However, with the ability to track or locate a specific individual comes the ability to profile and deliver targeted advertising or other specific services.

- Processing of sensitive data: As mentioned before, processing of biometric data could be used to determine sensitive data, in particular those with visual cues such as race, ethnic group or perhaps a medical condition.

- Revocability: an individual may easily change its facial appearance (beard, glasses, hat, etc.) which may be sufficient to fool facial recognition systems, especially when they operate in a non-controlled environment. However, the main facial features of an individual are stable in time and systems may also improve recognition by collecting and associating different known "faces" of an individual.

- Anti-spoofing protection: Many facial recognition systems are easy to spoof but manufacturers try to improve spoofing protection with techniques such as 3D imaging or video recording. However, most basic systems used in public applications do not include this type of protection.

Example:
An extreme imaginary example would be a next generation shopping centre video surveillance system that can recognise persons, automatically track movements, differentiate facial characteristics like smiles or anger. It could recognise regular customers entering the on-site car parking facility and route them to preferred parking places. When customers enter the shopping mall the system could identify clothes to suggest which stores to visit depending on available store offers, previous shopping history or from a predicted set of indicators. Customised advertising in shop windows or automatic denial of access to shops, restaurants and other places can also be arranged. Potential car thieves could be identified and tracked before they even touch a car. If needed tele-guided aerial vehicles (drones) with cameras and other sensors could keep track of suspects until the suspicion is diverted or confirmed. Objects hidden in clothing (knives or shoplifted items) could be detected. This technology is not only based on new biometric systems. It combines and processes information which is already available with other data from a range of different systems.

A similar application has been designed in the INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) project where technologies are combined to fight potential acts of terrorism and crime before it happens. The Working Party strongly emphasises that such use of biometrics would require

an appropriate legal basis and strict considerations regarding necessity and proportionality of such measures.

4.4.4. Voice recognition & combined uses

In addition to using voice recognition as a biometric for identification, a relatively common use involves the identification of specific features within the voice pattern to categorise the speaker. An example of this would be to analyse the responses of an individual throughout a telephone conversation to identify stress patterns and speech irregularities to highlight potential cases of fraud.

Testimonials published by manufacturers report that, by implementing such technology, financial services companies have increased fraud detection rates and enabled a faster service to settle genuine claims.

When used in a categorisation system the data protection risks are slightly different to a biometric identification system in that there should be no enrolment stage and no need for the long term storage of a biometric template. However, if a telephone conversation is recorded, as is typically the case with a financial institution, appropriate controls must be in place to ensure the security of these data.

- Accuracy: One data protection risk of such a system lies in the detection rates, specifically the false positive and false negatives, i.e. how many people are mistakenly identified as fraudulent or how many fraudulent claims are not identified? Whilst a categorisation system may be able to tolerate higher error rates than verification or identification there still must be appropriate processes in place to deal with those cases may be incorrectly categorised in a timely manner.

- Consent & Transparency: A privacy-friendly approach can be applied to such technologies such as taking care to ensure that calls were screened for suitability and data subjects informed of the process which was being undertaken. In one case study, individuals were deemed to be unsuitable for the trial if they did not speak English as a first language or had a disability to their hearing or cogitative function, or indeed, did not have access to a telephone. Claimants were free to decline to take part in the call and provide information in a traditional manner but also for those data subjects not wishing or not able, to participate in such a system without being disadvantaged.

- Further purposes or purposes of processing: Whilst the majority of instances of this technology would require specific infrastructure changes to implement as the public and private sectors consolidate their IT infrastructures to include technologies such as Voice over IP, voice recognition technologies may become easier to integrate without due regard to the data protection obligations of the controller.

- Revocability: if an individual can deliberately modify its voice, voice patterns are quite stable and may be efficient to uniquely identify an individual, in particular when the individual is not informed (and therefore not inclined to modify its voice).

- Anti-spoofing protection: recorded voices can be used to spoof voice recognition systems. Anti-spoofing techniques include questions/answers on contextual matters (by asking the date of the day or to repeat rare words).

4.4.5. DNA

The improvements of devices used for DNA sequencing and matching and the availability of equipment for DNA analysis at affordable prices makes it necessary to reconsider some of the assumptions of the previous working document on biometrics (WP80).

One of the major changes in DNA profiling technologies is the reduction in time required for the operations of DNA sequencing and matching. The continuous advances made over the years by academic research and biotechnology developers have reduced the time needed for the generation of a DNA profile from days to hours and even a fraction of an hour.

The kick-start of a market of DNA-based online services is a threat to individuals' rights to data protection especially when the service requires transfers of biometric samples and biometric data between different countries (including extra-EU countries), multiple data processors and the lack of appropriate safeguards for the processing of genetic or health data.

It is very likely that in the near future it will be possible to perform real-time (or near real-time) DNA profiling and matching of samples using portable devices, which will be the starting point for the development of DNA biometric identification/authentication systems with greater levels of accuracy compared to authentication done by fingerprints, voice and facial recognition.

DNA profiling improvements are also due to the increasing interest of governments, judges and law enforcement authorities in biotechnologies for criminal investigation. Because of the reliability of DNA matching and the fact that DNA samples can be collected without the data subject being aware of it, over the time several member states have created or started initiatives to create centralised data banks of DNA profiles related to convicted persons and samples found on crime scenes.

On May 2005, seven EU Member States signed the agreement known as "Prüm Treaty" to improve the cooperation in cross-border criminal investigations and justice by the means of exchange of information. The agreement sets new grounds in cooperation as it provides the signatories with certain rights of access to national DNA databases only in the repressive context (prosecution of crime), fingerprint data, personal and non-personal data, as well as vehicle registration data. Since then, more Member States have joined the Treaty and the essentials of the agreement were included in the Council Decision 2008/615/JHA.

Under this legal framework, several EU Member States have or will shortly have a functional national data bank with DNA profiles of convicted persons and crime scene evidences which raises some concerns about this specific data processing.

One of the major issues related to the creation of DNA data banks is the fact that the genetic data derived from DNA samples (loci) may reveal - not immediately during the collection phase - information associated with the health status, the predisposition to diseases or the ethnic origins. For this reason the creation of DNA databases pose a significant risk to human dignity and fundamental rights. This risk has been considered in the Council Resolution 2009/C 296/01. Specific provisions exist to limit DNA analysis to chromosome zones with no genetic expression by using a specific set of DNA markers not known to provide information about specific hereditary characteristics (this is also known as the so called "ESS" -European Standard Set).

However, the possibility that one of the markers extracted included in one national DNA database may reveal in the future some hereditary characteristics or other sensitive

information, requires a constant attention to developments in biology with the consequence that, in this unfortunate event, some of the information of the database should be deleted immediately. Additionally, because those DNA databases collect profiles of convicted persons, statistical analysis of the data should be strongly limited in order to avoid profiling based on sex or racial grounds.

As far as DNA databases for purposes of police and criminal justice are concerned, the European Court of Human Rights has ruled that a clear distinction should be made between the processing of personal data and genetic profiles of suspects and of persons convicted of a criminal offence[16].

There is also a potential risk that DNA analysis can be used to identify family members or relatives linked to unsolved crime or convicted persons, because the DNA profiles can be searched through the database using partial sets of markers or wild-cards. This functionality raises the issue about the implications of following up information derived from a familial search.

It should also be noted that there are specific risks related to the use of genome datasets in research contexts. The Working Party considers that access to the samples and data should be strictly restricted to the research community and permitted exclusively for research purposes; additionally, it is necessary to clarify under what circumstances research findings and results will be disclosed to the individuals (taking also into account their right not to know) or will be integrated into medical records.

Data protection risks associated with the use of DNA as a biometric can be described as follows:

- Accuracy: Even though DNA presents a very high-degree of accuracy, it should be taken into account that it will depend on the number of markers (loci) analysed. Testing systems should ensure the highest degree of accuracy.

- Impact: The use of DNA can be deemed as extremely intrusive for the individual. Genetic data may reveal sensitive information. Statistical analysis of the data may be used also for profiling and may have discriminatory effects for the persons concerned.

- Further purpose or purposes of processing: New technologies now permit increasing amounts of data exchange. For this reason it must be clear who may have access to the information of a DNA database. Familial searching and racial targeting can be deemed as a new technology challenging the original purpose of the processing in the currently available DNA databases.

- Consent & Transparency: Services are now being offered to carry out DNA analyses on biological samples sent through postal mail services (e.g. saliva) whose results are made available through the Internet. Insufficient identity checks could allow individuals or entities to submit samples from other individuals and getting sensitive personal data about other people as a result.

- Linkability: Given the amount and variety of information that can be derived from DNA sequencing, DNA provides high potential for misuse as the extracted data can be

[16] ECHR, judgment of 4.12.2008, S. and Marper vs. UK (Application nos. 30562/04 and 30566/04) in particular, paragraph 125.

easily linked with other databases allowing profiling of the individual. A familial search also allows creating links with relatives.

- Processing of sensitive data: DNA can reveal information associated with the health status, the predisposition to diseases or the ethnic origin of the individual. Applying the data minimisation principle when choosing the relevant loci is therefore of extreme importance. DNA information can be extracted from many samples for a longer period of time so it is advisable to ensure that access to the samples is strictly restricted to authorised users and for authorised uses only.

- Revocability: DNA is irrevocable.

- Anti-spoofing protection: DNA is, a priori, very difficult to spoof, however it is in many cases not difficult to collect samples of someone's DNA (e.g. hair) without his knowledge.

4.4.6. Signature biometrics

Signature biometrics can be deemed as an example of new uses of traditional biometric technologies. Signature biometrics are behavioural-based biometric techniques which measure the behaviour of a person as expressed by the dynamics of the handwritten signature. While traditional signature recognition relies on the analysis of static or geometric characteristics of the visual image of the signature (how the signature looks like), signature biometrics instead refer to the analysis of dynamic characteristics of the signature (how the signature was made) and this makes these techniques often referred as "dynamic signature".

Typical dynamic characteristics measured by a signature biometric system (such as a digitizing tablet) are the amount of pressure, the angle of writing, velocity and acceleration of the pen, formation of letters, direction of the signature strokes and other unique dynamic traits. These characteristics vary in use and importance from vendor to vendor and usually are collected using contact sensitive devices. Some signature recognition devices can perform verification by combining the analysis both static (the visual image) and dynamic (pressure, angle, velocity, etc.) characteristics of a signature.

Data protection risks associated with the use of signature biometrics can be described as follows:

- Accuracy: People may not always sign in the same manner, so they could face problems during the enrolment process as well as when verifying their identity.

- Impact: Biometrics based on behavioural characteristics such a signature may not be unique over time and can be changed by the data subject. Changes on signature can also have a physiological origin and can preclude a successful verification resulting in the need of alternative procedures in order to verify the identity of the individuals.

- Anti-spoofing : While the graphical image of a traditional signature can be easily replicated and forged by a trained human, photocopy or with computer graphics software, a dynamic signature is more secure because the verification process checks also dynamic characteristics which are complex and unique to the handwriting style of a person.

5. General Guidelines, Sector-Specific Recommendations and Technical and Organisational Measures.

The deployment of a biometric system relies on the cooperation of several actors:

- Manufacturers: to design and test biometric sensors and define the performance of biometric technologies;
- Integrators: to design the final product that will be sold to the customer: they choose the biometric technology and define partly the purposes of the system (by choosing which clients to address);
- Resellers: to commercialise the final product to the customer; they generally inform the client about the performance, the risks and potentially the legal framework;
- Installers: to install the product within the client's premises;
- Clients: to choose to buy a biometric system: they define the purpose and the means of the processing and are, therefore, data controllers;
- Data subjects: to provide biometric data used by the system.

Some actors fulfil one or more of the roles described above. Each role has a responsibility to ensure a privacy-friendly use of biometric systems: for instance, installer may not implement a security feature that the integrator defined.

5.1. General principles.

Regarding biometric data, security should be a primary concern because biometric data are irrevocable: therefore, a breach concerning biometric data threatens the further safe use of biometrics as identifier and the right to data protection of the concerned persons for which there is no possibility to mitigate the effects of the breach.

The risks increase with the number of applications using such data (especially the risks of breaches and of function creep). The more biometric data is used, the more likely biometric data theft will occur.

The Working Party recognises the current trend to allow for remote access to biometric systems, for example interfaces delivered over the internet. This trend introduces a new set of security problems many of which are well known to the IT industry. Deployment of such a system should involve appropriate technical security personnel from the IT industry early in the design phase.

The Working Party recommends a high level of technical protection for the processing of biometric data, using the latest technical possibilities. In this regard, the Working Party recommends following industry standards for the protection of the systems in which biometric information are processed.

5.2. Privacy by design

Privacy by design is the concept of embedding privacy proactively into technology itself.

Regarding biometric systems, Privacy by design concerns the whole value chain of biometric systems:

- manufacturers should implement Privacy by Design principles when they design new technologies and sensors: this can include the automatic deletion of the raw data after the template is calculated or the use of encryption for the storage of biometric data

(whether in a central database or on a smart card). Manufacturers should also concentrate on developing biometric technologies that are privacy-friendly;
- integrators and resellers should also implement Privacy by Design principles when they define the final product that will be sold, by choosing privacy-friendly technologies and adding security measures to the final product, such as the decentralization of the database;
- clients (prospective data controllers) should apply Privacy by Design principles whenever they request a specific biometric system or define the technical features of the system. In this case, manufacturers and integrators should offer a certain level of flexibility in their product in order to meet the principles of proportionality, purpose limitation, data minimisation and security.

These principles have already been successfully implemented into some biometric devices: some manufacturers have included in a specific biometric reader encryption features and anti-pulling and anti-tamper switches to prevent unauthorised access to biometric data.

The Working Party recommends that biometric systems are designed according to formal "development lifecycles" which include the following steps:

1. Specification of requirements based on a risk analysis and/or a dedicated Privacy Impact Assessment (PIA).
2. Description and justification on how the design fulfils the requirements.
3. Validation with functional and security tests
4. Verification of compliance of the final design with the regulatory framework

The Working Party encourages the definition of certification schemes that could ensure the implementation of Privacy by Design and reinforce the information of the data controllers about the data protection risks associated with biometric systems.

5.3. Privacy impact assessment framework

5.3.1. General principles

Privacy Impact Assessment (PIA) is a process in which an entity carries out an evaluation of the risks associated with a processing of personal data and a definition of additional measures designed to mitigate these risks. For example with RFID technology the Working Party has established that the entity that defines the application is responsible for the realisation of the PIA. This entity can be the data controller or the provider that designs the RFID application.

Because of the specific risks coming along with the use of biometric data, the Working Party recommends that the one that defines the purpose and the means of the device execute privacy impact assessments as an integral part of the design phase of systems dealing with this type of data. It can be the manufacturer, the integrator or the final client.

The PIA should take into account:

- The nature of the collected information,
- The purpose of the collected information,
- The accuracy of the system, assuming that important decisions could derive for an individual from a match/not match of a biometric pattern,
- The legal basis and legal compliance; is consent required?

- The access to the device and the internal and external sharing of information within the data controller, which will imply security techniques and procedures to protect personal data unauthorised access,
- The less privacy-invasive measures already taken. Is there an alternative procedure to the biometric device (like asking for the I.D. card)?
- The decisions taken regarding retention time and deletion of data. What is the relevant period of time? Are all data collected for the same period of time? Is there an automatic decision mechanism and appropriate fall-back process?
- The data subjects' rights.

Privacy impact assessments should not be only focussed on identifying the risks, they should also provide with adequate data protection measures and how the data controller has come out with appropriate solutions to mitigate the data protection risks identified in the previous section.

When the PIA has been conducted by the manufacturer or the integrator, the deployment of the biometric system can also require an additional assessment to take into account the specificities of the data controller. For instance, when a biometric system is integrated in the client's information system, the client should realise an additional PIA that consider its own IT security measures and procedures.

5.3.2. The specificity of biometric data

Biometric data require specific attention because they unambiguously identify an individual by using its unique behavioural or physiological characteristics.

For this reason PIAs should aim to assess how the three following risks can be avoided or substantially limited by the system it analyses.

The first risk is identity fraud, especially in the case of identification and authentication. The biometric device should not be fooled by a spoofing attack and ensure that the person who is attempting to perform the matching really is the person that is registered in the system. That threat seems less meaningful for biometric data that cannot be collected without the knowledge the data subject, such as the vein pattern[17]. It is however a major issue for fingerprint or facial recognition devices. Fingerprints are left everywhere by simply touching any object. The face can also be captured by a photo without the person being aware of it.

The second risk is the purpose diversion either by the data controller itself or by a third-party including law enforcement authorities. This common threat regarding personal data becomes a crucial one when biometric data are used. Manufacturers should take all security measures to avoid any improper use of the data and make sure that any data that are not needed anymore for the purpose of the processing are deleted immediately.

As with any other data, legitimately processed or stored biometric data or the sources of biometric may not be processed or enrolled by the controller for any new or other purpose unless there is a new legitimate ground for this new processing of these data.

[17] Even if it is difficult to predict which attacks on vein pattern technology will be possible in the coming years if this technology is more widely used.

The third risk is data breach that requires in the biometric data context special actions depending on which kind of data have been compromised. If a system is used that creates biometric data based on an algorithm that converts a biometric template into a certain code and either the biometric data or the algorithm is stolen or compromised they need to be replaced. When a data breach involves the loss of directly identified biometric data that are very close to the source of biometric data such as pictures of faces or fingerprints, the concerned person needs to be notified in detail in order to be able to defend himself in a possible future incident where these compromised biometric data may be used against him as evidence.

5.4. Technical and Organisational Measures

On account of their nature, the processing of biometric data requires special technical and organisational measures and precautions to prevent adverse effects to the data subject in the event of a data breach - in particular because of the risks of unlawful conduct resulting into the unauthorised "reconstruction" of a biometric feature from the reference template, their interlinking with different databases, their further "use" without the data subjects knowledge for non-compatible purposes with the original ones and/or the possibility that some biometrics data could be used to reveal racial or health information about subjects.

5.4.1. Technical Measures

- *Use of biometric templates*

Biometric data should be stored as biometric templates whenever that is possible.

Template should be extracted in a way that is specific to that biometric system and not used by other controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation.

- *Storage on a personal device vs. centralised storage*

Whenever it is permitted to process biometric data, it is preferred to avoid the centralised storage of the personal biometric information.

Especially for verification, the Working Party considers advisable that biometric systems are based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices). Their biometric features can be compared with the template(s) stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including biometric information should be, in general and if possible, avoided. Indeed, if the card and/or device is lost or mislaid, there are currently limited risks that the biometric information they contain may be misused. To reduce the risk of identity theft, limited identification data related to the data subject should be stored in such devices.

However, for specific purposes and in presence of objective needs centralised database containing biometric information and/or templates can be considered admissible. The biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable. Mechanisms based on cryptographic technologies, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used.

When the biometric data are stored on a device that the data subject physically controls, a specific encryption key for the reader devices should be used as an effective safeguard to protect these data from unauthorised access. Furthermore such decentralised systems provide

for a better protection of the biometric data by design as the data subject stays in physical control of his biometric data and there is no single point that can be targeted or exploited.

The Working Party also stresses out that the idea of centralised database covers a wide range of technical implementations from the storage within the reader to a network hosted database.

- *Renewability and revocability*

As the source of biometric data cannot be changed biometric systems whose purpose is to establish an identity link must be designed in a way that the enrolment process and the processing of biometric data allows that multiple and independent biometric templates can be extracted from the same source in order to be able to replace them in the case of a data breach or a technological evolution.

Biometric systems should be designed in a way that allows to revoke the identity link, either in order to renew it or to permanently delete it e.g. when the consent is revoked[18].

- *Encrypted form*

As for the security issue, adequate measures should be adopted to safeguard the data stored and processed by the biometric system: biometric information must always be stored in encrypted form. A key management framework must be defined to ensure that the decryption keys are only accessible on a need to know basis.

Given the widespread use of public and private databases containing biometric information and the increasing interoperability of different systems using biometrics, the use of specific technologies or data formats that make interconnections of biometric databases and unchecked disclosures of data impossible should be preferred.

- *Anti-spoofing*

To maintain the reliability of a biometric system and prevent identity fraud the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not, for example, a picture tied on an impostor's head.

- *Biometric encryption and decryption*

Biometric encryption is a technique using biometric characteristics as part of the encryption and decryption algorithm. In this case, an extract from biometric data is generally used as a key to encrypt an identifier needed for the service.

This system has many advantages[19]. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored. Moreover, the personal data is revocable as it is possible to create another identifier that can

[18] For example the TURBINE technology that is aimed to protect the biometric template by cryptographic transformation of the fingerprint information into a non-invertible key that allows matching by bit-to-bit comparison. The transformed biometric data is considered irreversible to the biometric samples and original templates. Moreover, to enhance user trust, this key will also be revocable, i.e. a new independent key can be generated to re-issue biometric identities. See also: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

be protected with biometric encryption as well. Finally, this system is more secure and easier to use to the person: it solves the problem to remember long and complex passwords.

However, the cryptographic problem to overcome is not easy because encryption and decryption are intolerant to any changes in the key, whereas biometric provides different pattern which may give rise to changes in the extracted key. The system must therefore be able to compute the same key from slightly different biometric data, without increasing the False Acceptance Rate.

The Working Party agrees that Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

- *Automated data erasure mechanisms*

In order to prevent that biometric information are stored for longer than is necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system.

When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore no biometric database remains when the reader is sold or uninstalled. Anti-pulling switches may also be used to automatically erase the data if someone tries to steal the reader.

- *Large biometric databases and "weak link" databases*

Some countries are using large biometrics databases, mainly for two purposes: help criminal investigations and secure the delivery of identity papers (passports, identity card, driving licenses). The databases used for criminal investigation generally gather information about criminals and suspects and must be designed in order to identify a person with the biometric data. In the contrary, databases used to combat identity fraud include biometric data of the whole population and should only be used to authenticate the person (for instance if the person has lost its papers or destroyed the secure chip of the passport in which the biometric data is stored).

When a central database is used for the purpose of the struggle against identity fraud, the Working Party considers that technical measures must be implemented to avoid any purpose diversion. First, the data minimisation principle demands that only the data necessary to authenticate the person must be collected. For instance, it is considered that the comparison of the fingerprints of two fingers is precise enough to authenticate a person.

Moreover, data controllers can use "weak link" databases where the identity of a person is not linked to a single biometric data set but rather to a group of biometric data set. The design of the database should guarantee the authentication of the person with a very good probability (for instance 99.9% which is sufficient to dissuade fraudsters) and make sure the database cannot be used for identification (because one biometric data set corresponds to a large number of persons).

The Working Party supports the use of such systems when large biometric databases are used for the purpose of struggle against identity fraud.

Example: technical measures for authentication systems
The source of biometric data is unique and potentially lifelong associated with the data subject. If it is used as basis for authentication systems it must be kept in mind that it cannot be changed whereas in common authentication technologies that typically require 'to know or to own' a credential (e.g. user ID, password) a change of that credential is always possible. Therefore, systems using biometric authentication must implement special safeguards to protect the link between biometric and other identity data:
- Template data should not be centrally stored since the security of the biometric data storage is essential with regard to the overall security of the biometric system. A distributed storage (e.g. on a smartcard) should be preferred. In that case both the source of the data and the template are carried by the data subject.
- Storage and transmission of biometric data have to be protected against interception, unauthorised disclosure and modification through the use of appropriate cryptographic technologies.
- Some types of biometric data are not secret (e.g. the face) and cannot be locked, blocked or changed after data breaches, disclosures or cases of misuse. As a consequence, authentication should be combined with other lockable or changeable credentials.

5.4.2. Organisational measures

To guarantee data protection, organisational measures must be planned and executed. For instance, the data controller has to establish a clear procedure on who can access the information on the system, if the access is partial or not, and for what reasons. All actions would have to be tracked.

The Working Party observes that outsourcing to external service providers is possible including for visa applications (Sections 13 and 43 of Regulation (EC) no 810/2009 of 13 July 2009 establishing a Community Code on Visas) and is becoming more popular because of the more frequent use of cloud storage.

In that case, the data controller has to establish a detailed policy on how to control its contractors such as unexpected inspections, and require guarantees regarding employees, procedure regarding individual’s rights etc.

Done at Brussels, on 27 April 2012

For the Working Party
The Chairman
Jacob KOHNSTAMM