ARTICLE 29 DATA PROTECTION WORKING PARTY

00727/12/EN
WP 192

Opinion 02/2012 on facial recognition in online and mobile services

Adopted on 22 March 2012

1. Introduction

There has been a rapid increase in the availability and accuracy of facial recognition technology in recent years. Furthermore this technology has been integrated into online and mobile services for the identification, authentication/verification or categorisation of individuals. The technology, once the subject of science fiction, is now available for use by both public and private organisations. Examples of use in online and mobile services include social networks and smartphone manufacturers.

The ability to automatically capture data and recognise a face from a digital image has been considered previously by the Article 29 Working Party (WP29) in the Working document on biometrics (WP80) and the recently published Opinion 03/2012 (WP193) on developments in biometric technologies. Facial recognition is considered within the scope of biometrics as, in many cases, it contains sufficient detail to allow an individual to be uniquely identified.

Opinion 03/2012 comments that:

> *"[biometrics] 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 statement is particularly true in the case of facial recognition in online and mobile services when images of an individual may be captured (with or without the individual being aware) and then transmitted to a remote server for further processing. Online services, many owned and operated by private organisations, have built up vast collections of images uploaded by the data subjects themselves. In some cases these images may also be unlawfully obtained by scraping other public sites such as search engine caches. Small mobile devices with high resolution cameras enable users to capture images and link in real-time to online services through always-on data connections. As a result users are able to share these images with others or perform identification, authentication/verification or categorisation to access additional information about the known or unknown person standing before them.

Facial recognition in online and mobile services therefore requires specific attention from WP29 as the use of this technology presents such a range of data protection concerns.

The purpose of this opinion is to consider the legal framework and provide appropriate recommendations applicable to facial recognition technology when used in the context of online and mobile services. This opinion addresses European and national legislative authorities, data controllers and users of such technologies. The opinion does not intend to repeat the principles referred to in Opinion 03/2012 but rather builds upon them within the scope of online and mobile services.

2. Definitions

Facial recognition technology is not new and a range of definitions and interpretations of the terminology exist. It is therefore helpful to clearly define the technology as addressed by this opinion.

Digital image: A digital image is a representation of a two-dimensional image in a digital form. However, recent advances in facial recognition technology require that three-dimensional images are included in addition to both static and moving images (i.e. photographs, recorded and live video).

Facial recognition: Facial recognition is the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorisation[1] of those individuals. The process of facial recognition itself is comprised of a number of discrete sub-processes:

a) Image acquisition: The process of capturing the face of an individual and converting to a digital form (the digital image). In an online and mobile service the image may have been acquired in a different system, e.g. taking a photograph with a digital camera which is then transferred to an online service.

b) Face detection: The process of detecting for the presence of a face within a digital image and marking the area.

c) Normalisation: The process to smooth variations across detected facial regions, e.g. converting to a standard size, rotating or aligning colour distributions.

d) Feature extraction: The processing of isolating and outputting repeatable and distinctive readings from the digital image of an individual. Feature extraction can be holistic[2], feature-based[3] or a combination of the two methods[4]. The set of key features may be stored for later comparison in a reference template[5].

e) Enrolment: If this is the first time an individual has encountered the facial recognition system the image and/or reference template may be stored as a record for later comparison.

f) Comparison: The process of measuring the similarity between a set of features (the sample) with one previously enrolled in the system. The main purposes of comparison are identification and authentication/verification. A third purpose of comparison is categorisation which is the process of extracting features from an image of an individual in order to classify that individual in one or several broad categories (e.g. age, gender, colour of clothes, etc). It is not necessary for a categorisation system to have an enrolment process.

3. Examples of facial recognition in online and mobile services

Facial recognition can be incorporated into online and mobile services in a number of different ways for a variety of purposes. In the context of this opinion the WP29 focuses on a number of different examples which aim to provide additional context to the legal analysis and include the use of facial recognition for identification, authentication/verification and categorisation purposes.

---

1 Identification, authentication/verification and categorisation are defined in 03/2012

2 Holistic feature extraction: a mathematical representation of the whole image such as that resulting from principal component analysis

3 Feature-based feature extraction: identifying locations of specific facial features such as eyes, nose and mouth

4 Also known as a hybrid feature extraction method

5 Template is defined in 03/2012 as "*Key features 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.*"

3.1. Facial recognition as a means of identification

Example 1: A social networking service (SNS)[6] allows users to attach a digital image to their profile. Furthermore users are able to upload images to share with other registered or non-registered users. Registered users can manually identify and tag other individuals (who may or may not be a registered user) within the images they upload. Such tags may be viewed by the tag creator, shared with a broader group of friends or shared to all registered or non-registered users. The SNS is able to use the tagged images to create a reference template for each registered user and, through the use of a facial recognition system, automatically suggest tags for new images as they are uploaded.

Those images of individuals which are made publically available by users could then be accessed and cached by an internet search engine. The search engine may wish to enhance their search feature by allowing users to provide an image of an individual and return results of close matches and also link back to the SNS profile page. The query image may be captured direct from a smartphone camera.

3.2. Facial recognition as a means of authentication/verification

Example 2: A facial recognition system is used to replace a username/password to control access to an online or mobile service or device. During enrolment, a camera on the device is used to acquire an image an authorised user of the device and a reference template created which could be stored on the device or remotely by the online service. To gain access to the service or device, a new image is acquired of the individual attempting access and compared to the reference image. Access is granted if the system determines a positive match.

3.3. Facial recognition as a means of categorisation

Example 3: The SNS described in Example 1 may licence access to the image library to a third-party who operates an online facial recognition service. The service allows customers of the third-party to incorporate facial recognition technology into other products. The functionality allows these other products to submit images of individuals for the purpose of detecting and categorising faces into a set or pre-defined criteria; e.g. likely age, gender and mood.

Example 4: A games console uses a gesture control system where movements of the user are detected in order to provide controls to the game. The camera(s) used for the gesture control system share images of individuals with a facial recognition system which predicts the likely age, gender and mood of the game players. Data, including that from other multi-modal factors, may then alter the game play to enhance the user experience or to change the environment to reflect the user's predicted profile. In a similar manner, a system could classify users to allow/deny access to age-related content or to display in-game targeted advertising.

4. Legal Framework

The relevant legal framework for facial recognition is the Data Protection Directive (95/46/EC) which has been discussed in this regard in Opinion 03/2012. This section aims only to give a summary of the legal framework in the context of facial recognition in online and mobile services, based on the examples provided in Section 3. Further examples of facial recognition are considered in Opinion 03/2012.

[6] A social network service is broadly defined in Opinion 05/2009 on online social networking as "*an online communication platform which enables individuals to join or create networks of like-minded users*"

4.1. Digital images as personal data

When a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data. This will be dependent on a number of parameters such as the quality of the image or the particular viewpoint. Images of scenes containing individuals in the distance or where the faces are blurred are unlikely to be considered personal data in most cases. It is however important to note that digital images may contain the personal data of more than one individual (e.g. in Example 4, multiple players may be in the frame) and the appearance of others in the photograph may imply an existing relationship.

Opinion 04/2007 on the concept of personal data reiterates the point that if data refers to "*characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*" then this is also considered as personal data.

By definition, a reference template created from an image of an individual is also personal data as it contains a set of distinctive features of an individual's face which is then linked to a specific individual and stored for reference for future comparison in identification and authentication/verification.

A template or set of distinctive features used only in a categorisation system would not, in general, contain sufficient information to identify an individual. It should only contain sufficient information to perform the categorisation (e.g. male or female). In this case it would not be personal data provided the template (or the result) is not associated with an individual's record, profile or the original image (which will still be considered personal data).

Furthermore as digital images of individuals and templates relate to the "*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*[7]" they should be considered as biometric data.

4.2. Digital images as special categories of personal data

Digital images of individuals may in some specific cases be considered as a special category of personal data[8]. Specifically where digital images of individuals or templates are further processed to derive special categories of data, they would certainly be considered within this category. For example, if they are going to be used to obtain ethnic origin, religion or health information can be derived.

---

7 Definition of biometrics data from Opinion 03/2012

8 Case law in certain countries has classed digital images of faces as special categories of data – LJN BK6331 Dutch High Court 23 March 2010

4.3. Processing of personal data in the context of a facial recognition system

Facial recognition relies on a number of automated processing stages as previously described. Therefore, facial recognition constitutes an automated form of processing of personal data, including biometric data.

Through the use of biometric data, facial recognition systems may be subject to additional controls or other legislation in individuals Member States such as prior authorisation or employment law. The use of biometrics in an employment context in considered further in Opinion 03/2012.

4.4. Data controller

Using the provided examples, data controllers will typically be website owners and/or online service providers as well as mobile application operators who engage in facial recognition in that they determine the purposes and/or means of the processing[9]. This will include the conclusion drawn in Opinion 05/2009 on online social networking which states that "SNS providers are data controllers under the Data Protection Directive".

4.5. Legitimate ground

Directive 95/46/EC lays down the conditions with which the processing of personal data must comply. This means that the processing must first be compliant with data quality requirements (Article 6). In this case the digital images of individuals and the respective templates must be "relevant" and "not excessive" for the purposes of the facial recognition processing. Furthermore, the processing may only be performed if one of the criteria specified in Article 7 is fulfilled.

Because of the particular risks involved with biometric data, this is will therefore require the informed consent of the individual prior to commencing the processing of digital images for facial recognition. However, in some cases, the data controller may temporarily need to perform some facial recognition processing steps precisely for the purpose of assessing whether a user has provided consent or not as a legal basis for the processing. This initial processing (i.e. image acquisition, face detection, comparison, etc) may in that case have a separate legal basis, notably the legitimate interest of the data controller to comply with data protection rules. Data processed during these stages should only be used for the strictly limited purpose to verify the user's consent and should therefore be deleted immediately after.

In Example 1, the data controller has determined that all new images uploaded by registered users of the SNS should undergo face detection, feature extraction and comparison. Only those registered users who have a reference template enrolled in the identification database will match against these new images and therefore have a tag suggested automatically. If the consent of the individual was to be considered as the only possible legitimate basis for all processing the entire service would be blocked as, for example, there is no means to gain consent of non-registered users who may have their personal data processed during face detection and feature extraction. Furthermore it would not be possible to distinguish between the faces of registered users who had and had not consented without first performing facial recognition. Only after identification has taken place (or a failure to identify) would a data controller be able to determine whether or not they have the appropriate consent for the specific processing.

[9] See Opinion 01/2010 on the concepts of "controller" and "processor"

Prior to a registered user uploading an image to the SNS they must first be clearly informed that these images will be subject to a facial recognition system. More importantly, registered users must also have been given a further option as to whether or not they consent to their reference template to be enrolled into the identification database. Non-registered users and registered users who have not consented to the processing will therefore not have their name automatically suggested for a tag because images in which they appear will produce a "no-match" result.

Consent given by the image uploader should not be confused with the need for a legitimate basis for the processing of personal data of other individuals who may appear in the image. To this end, the data controller may wish to apply a different legitimate ground for processing for the intermediate stages (face detection, normalisation and comparison) such as it being in the legitimate interest of the data controller, provided that sufficient restrictions and controls are in place to protect the fundamental rights and freedoms of the data subjects who are not the uploader of the image. Such controls would include ensuring that no data resulting from the processing is retained once a no-match result has been obtained (i.e. all templates and associated data are securely deleted). The data controller may also wish to consider providing tools to their users which allow for the image uploader to blur the faces of those individuals who fail to match against a template in the reference database. Enrolment of an individual's template into an identification database (therefore enabling a match result and subsequent tagging suggestions) would only be possible with the informed consent of the data subject.

In Example 2, there is a clear opportunity to gain the consent of the individual authorised to access the device during the enrolment process. In order for the consent to be valid, an alternative, and equally secure, access control system must be in place (such as a strong password). This alternative privacy friendly option should be the default. Where an individual user presents themselves before a camera connected to the device for the explicit purpose of gaining access then, we can consider that this individual has provided consent for the resulting facial data processing needed for authentication, even if that individual is not an authorised user of the device. However, the level of information provided must still be sufficient to ensure the consent is valid.

The further enhancement to the SNS photo library described in Example 3 would be a clear case of a breach of purpose limitation and therefore valid consent must be given by the individual prior to the introduction of such a feature clearly indicating that such processing of images will take place. This is also the case of the search engine described in Example 1. The images obtained by search engine were displayed with the intention for viewing and not for acquisition by a facial recognition system. The search engine provider would be required to obtain consent from the data subjects to be enrolled into the second facial recognition system.

This would also be the case in Example 4 as the user may not expect the images acquired for the gesture-control to be subject to further processing. If the data controller is requesting consent for processing on a longer-term (i.e. over time or across games) the data controller must provide regular reminders to users that the system is operating and be switched-off by default.

Opinion 15/2011 on the definition of consent considers the quality, accessibility and visibility of information relating to the processing of personal data. The opinion states:

> *"information must be given directly to individuals. It is not enough for information to be "available" somewhere."*

Therefore, information relating to the facial recognition feature of an online or mobile service should not be hidden but be available in an easily accessible and understandable way. This will include ensuring that the cameras themselves are not operating in a covert manner. Data controllers should take into account the public's reasonable expectations of privacy when implementing facial recognition technology and address these concerns appropriately.

In this context, consent for enrolment cannot be derived from the general user's acceptance of the overall terms and conditions of the underlying service unless the primary aim of the service is expected to involve facial recognition. This is due to the fact that, in most cases, enrolment will be an additional feature and not directly related to the operation of the online or mobile service. Users may not necessarily expect that such a feature is activated when using the service. To this end, users should be explicitly provided with the opportunity to provide their consent for this feature either during registration or at a later date, depending on when the feature is introduced.

In order to consider the consent valid, adequate information about the data processing must have been given. Users should always be provided with the possibility to withdraw consent in a simple manner. Once consent is withdrawn processing for the purposes of facial recognition should stop immediately.

5. Specific risks and recommendations

The risks to privacy from a facial recognition system will depend entirely on the type of processing involved and purpose(s). There are however, certain risks which are more relevant at specific stages of facial recognition. The following section highlights the major risks and provides relevant best practice recommendations.

5.1. Unlawful processing for the purposes of facial recognition

In an online setting, images can be acquired by the data controller in many ways such as provided by the users of the online or mobile service, their friends and colleagues or from a third party. Images may contain the faces of the users themselves and/or other registered or non-registered users or acquired without the knowledge of the data subject. Regardless of the means by which these images may be acquired a legal basis is required to process them.

Recommendation 1: If the data controller is acquiring the image directly (e.g. as in Examples 2 and 4) then they must ensure they have the valid consent of the data subjects prior to acquisition and provide sufficient information relating to when a camera is operating for the purpose of facial recognition.

Recommendation 2: If individuals are acquiring digital images and uploading them to online and mobile services for the purpose of facial recognition the data controllers must ensure that the image uploaders have consented to the processing of the images which may take place for the purposes of facial recognition.

Recommendation 3: If data controllers are acquiring digital images of individuals from third parties (e.g. copied from a website or purchased from a different data controller) they must carefully consider the source and the context in which the original images are acquired and processed only if the data subjects had consented to such processing.

Recommendation 4: Data controllers must ensure that digital images and templates are only used for the specified purpose for which they have been provided. Data controllers should put technical controls in place in order to reduce the risk that digital images are further processed by third parties for purposes for which the user has not consented to. Data controllers should put in place tools for users to control the visibility of their images that they have uploaded where the default is to restrict access by third parties.

Recommendation 5: Data controllers must ensure that digital images of individuals who are not registered users of the service or have otherwise not consented to such processing are only processed in so far as the data controller has a legitimate interest for such processing. For example, in the case of Example 1, to stop processing and deleting all data in the case of a no-match result.

Security breach during transit

In the case of online and mobile services it is likely that there will be data transit between image acquisition and the remaining processing stages (e.g. uploading an image from a camera to a website for feature extraction and comparison).

Recommendation 6: The data controller must take appropriate steps to ensure the security of data transit. This may include encrypted communication channels or encrypting the acquired image itself. Where possible, and especially in the case of authentication/verification, local processing should be favoured.

5.2. Face Detection, Normalisation, Feature Extraction

Data minimisation

Templates generated by a facial recognition system may contain more data than are necessary to perform the specified purpose(s).

Recommendation 7: Data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Templates should not be transferrable between facial recognition systems.

Security breach during data storage

Identification and authentication/verification are likely to require the storage of the template for use in a later comparison.

Recommendation 8: The data controller must consider the most appropriate location for storage of the data. This may include on the user's device or within the data controller's systems. The data controller must take appropriate steps to ensure the security of the data stored. This may include encrypting the template. It should not be possible to obtain unauthorised access to the template or storage location. Especially for the case of facial recognition for the purpose of verification, biometric encryption techniques may be used; with these techniques, the cryptographic key is directly bound to the biometric data and is re-created only if the correct live biometric sample is presented on verification, whereas no image or template is stored (thus forming a type of "untraceable biometrics").

Subject access

Recommendation 9: The data controller should provide the data subjects with appropriate mechanisms to exercise their right of access, where appropriate, to both the original images, and the templates generated in the context of facial recognition.

Done at Brussels, on 22 March 2012

For the Working Party
The Chairman
Jacob KOHNSTAMM