•

3.22. Facial recognition

3.22.1. Description of threat

Facial recognition is the process by which a person can be identified or otherwise recognised from a digital image. Facial recognition can occur in one of two ways:

1. Identification – The identity of an individual is recognised within a digital image, usually made by comparing the test image with a template derived during an enrolment phase

2. Categorisation – The presence of an individual is recognised within a digital image and a categorisation is made on identifiable features such as age, gender or weight. This may not require an enrolment phase as test images are compared to a pre-calculated template for example, a statistical representation of the average for that category

Identification would not necessarily need to be tied to a real-world identity. It could also be used to identify repeat visitors to premises.

The accuracy of the system is critical when considered to the purpose. For example, a system for delivering targeted advertising based on gender will tolerate a much lower accuracy than an eBorder control system. In the former, if the system cannot determine the gender (e.g. subject is wearing a hat or in poor lighting) then it could select a non-targeted advertisement. If an eBorder control system was unable to identify an individual a manual intervention would be required causing delay. In the worst case scenario, a misidentification could grant access to an unauthorised individual.

In a number of cases the link between an individual's photograph and name may not be classed as high risk personal data but clearly could lead to other, potentially sensitive data, being disclosed. The obvious examples being race or ethnic origin or physical or mental health.

3.22.2. Applicable data protection principles

This is a threat to an individual's right to have their data processed for purposes that they did not consent or for purposes they were not sufficiently made aware

This is a threat to an individual's right to have their data protected against unauthorised or unlawful processing and against accidental loss, destruction or damage

This is a threat to an individual's right of access to their personal data, the purposes of processing and details of the recipients of that data

This is a threat to an individual's right to ensure that no decision which significantly affects them is based solely on processing their personal data by automatic means

3.22.3. Threat scenarios

- Large repositories of photographs in the hands of private companies could be requested by law enforcement officials to identify participants of public disorder.
- Private companies create repositories of photographs from CCTV images to identify previous customers. Individuals may be profiled into categories such as high spender or suspected shoplifter
- Advertising hoardings fitted with facial recognition software present targeted advertising to passing individuals. This could be based of categorisation (i.e. age, gender) or identification
- A supermarket uses facial recognition software to identify where customers focus their attention whilst shopping in the store
- An organisation uses facial recognition software to track customers through the establishment for queue management or other internal process

3.22.4. Impact

The controlled use of a facial recognition system such as eBorder control would only impact upon those who have registered and use the system. However, the technology is as such a state where facial recognition could be incorporated with current CCTV systems in private premises for a range of applications.

3.22.5. Likelihood

A number of online services are offering facial recognition services. Notably both Facebook and Google's Picasa allow for the automatic recognition and tagging of individuals in photographs. In addition, the online company Face.com offers developers free access to its facial recognition algorithm through its API[79]. Access to an effective and efficient algorithm to third-party developers will allow for a range of services to be made available.

[79] http://developers.face.com/

Recent reports[80] suggest that the FBI and NSA are scraping images from the web in order to create a large database to support facial recognition surveillance capabilities.

3.22.6. Mitigation

In the case of categorisation there is unlikely to be a business need to store the test image once the categorisation has been made. Assuming that this is the case and notification is given to the data subject, where appropriate, there may be few threats to information rights outside of those already mentioned in respect of hidden personalisation (Section 3.21) and natural user interfaces (Section 3.20). However, even if appropriate visual cues are available it must be clear to data subjects what processing is taking place. For example, if a video camera is visible this could be for constant recording, categorisation or identification.

3.22.7. Action by the ICO

- Liaison with key technology stakeholders.

[80] http://www.dailymail.co.uk/news/article-2645304/New-report-says-NSA-intercepting-millions-images-day-create-facial-recognition-database.html