ReedSmith

Client Alert

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this Alert, please contact the author:

Cynthia O'Donoghue
Partner, London
+44 (0)20 3116 3494
codonoghue@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

The Article 29 Working Party publishes Opinion 02/2012 on the use of facial recognition technology in mobile and online services, highlighting the data protection considerations in its recommendations

In the midst of a rapid increase in the availability and accuracy of facial recognition technology in recent years, the Article 29 Working Party adopted adopt in March this year Opinion 02/2012, highlighting the data protection considerations on the use of facial recognition technology in services such as social networking and for smartphones.

The Working Party's opinion states that facial recognition is considered to be within the scope of biometrics as there would be sufficient detail to allow an individual to be uniquely identified. Defined as the "*automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/ verification or categorisation of those individuals*", the facial recognition process comprises a number of discrete sub-processes including image acquisition, face detection, feature extraction, enrolment and comparison. Examples where facial recognition is being used in online and mobile services include:

- A social networking site allowing users to upload images and tag them - the social networking site is then able to use the tags in those images to create a reference template for each registered user, and through facial recognition automatically suggest tags for new images as they are uploaded
- Facial recognition used to replace a username/ password logon to an online or mobile service or device (similar to Samsung Galaxy Nexus 'Face Unlock' software)

The Working Party found that a digital image would constitute personal data if it contained "*an individual's face which is clearly visible and allows for that individual to be identified*", but this would be dependent on factors such as quality of the image. Images containing persons in the distance or with blurred faces are unlikely to be personal data, although can contain the personal data of more than one person. A previous Working Party Opinion stated 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 it is considered personal data. Furthermore, a reference recognition 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 the individual and stored for reference.

The Working Party continued that in specific cases some digital images that are further processed to determine ethnic origin, religion or health information, or facial recognition reference templates that are stored for comparison purposes, may constitute sensitive data.

Where facial recognition technology is involved, data controllers will typically be the website owners, the online service providers and/or the mobile application operators who engage in facial recognition, and the processing of such data must be compliant with data quality requirements. Because of the particular risk surrounding biometric data, informed consent is required before processing digital images for facial recognition. However, "initial processing" by the data controller (acquiring the image, fact detection and comparison, etc) in order to assess whether a user has provided consent or not will fall into the "legitimate interest", and can be performed without consent.

The Working Party gave the following best practice recommendations on how to address specific risks related to facial recognition technology:

- To avoid unlawful processing, data controllers acquiring images from users directly and processing these images, should obtain the valid consent of users
- Data controllers should implement appropriate security measures to: (a) reduce the risk that digital images are further processed by third parties for purposes not covered by the user's consent; (b) allow users to control visibility of their images; (c) ensure that data transit between acquisition and processing is secure; and (d) store the recognition template using appropriate encryption means
- Data controllers must ensure that the data extracted to build a template will not be excessive and will only extend to information required for that purpose
- Data controllers should provide users with appropriate mechanisms to exercise access rights relating to both the original images and the templates generated in the context of facial recognition

- Users should have the opportunity to withdraw their consent, at which point processing should cease immediately

A full copy the press release can be found here and the full Working Party Opinion 02/2012 can be found here.