FACIAL RECOGNITION: FACING THE FUTURE

'Facial recognition' is a technique which uses technology to identify individuals from digital images of individuals' faces. As use of this technology has grown, so too has the controversy surrounding it, particularly when used 'live' (ie. using technology which scans and identifies individuals' faces in real time).

Attitudes to the use of facial recognition and other biometric identification techniques vary across the world, in line with cultural norms. Organisations planning to use biometric identification techniques such as facial recognition should think carefully about the potential impact on the individuals concerned, and check that the use is compliant with applicable laws. Steaming ahead without first checking the law could result in large fines and reputational damage.

"Organisations wishing to make use of CCTV and/or biometric identification techniques such as facial recognition should: conduct thorough risk assessments to analyse the impact on the individuals involved; consider which laws will apply; inform the relevant data protection regulator(s) and pay any relevant fee to the regulator(s); and take advice where necessary."

Treatment around the world

Rules on the use of facial recognition across the world reflect different cultural approaches to the right to privacy. For example, we understand that in 2019 the city of San Francisco banned facial recognition,[1] but that the technique is relatively common in China. In Europe, the authorities are particularly suspicious of facial recognition and biometric identification techniques. For example, a Swedish high school was recently fined the equivalent of £16,800 by the country's data protection authority for employing facial recognition technology to track students' attendance.[2] The French privacy watchdog warned high schools in the south of France against instituting a similar scheme, stating that it considered it *"neither necessary nor proportionate"*.[3] Meanwhile, the UK Information Commissioner's Office ("ICO") last year conducted an investigation into the installation of two facial recognition cameras in London's King's Cross,[4] following which King's Cross announced that it had abandoned plans to use the technology in the future.

At European Union level, the European Commission has declared that it generally considers that any processing of biometric data, including facial recognition technology, is prohibited in principle by data protection laws, unless it falls into a specific set of exceptions, is duly justified, proportionate and subject to appropriate safeguards. As a result, it has announced that it will launch *"a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards."* [5]

The GDPR

The use of biometric identification techniques is currently governed by the EU General Data Protection Regulation ("GDPR") and, in the UK, also the Data Protection Act 2018 ("DPA").

Under the GDPR, facial images are considered 'biometric data'. 'Biometric data' can include a wide variety of information, from fingerprints to the analysis of the way that individuals move ('gait analysis'), or technologies using eye tracking ('gaze analysis'). When used for the purpose of *"uniquely identifying a natural person"*, biometric data are one of the 'special categories' of personal data. These must not be processed at all unless one of the following applies:[6]

- The data subject has given their explicit consent;
- Processing is necessary to fulfil employment or social security rights and obligations;
- Processing is necessary to protect the vital interests of the data subject (eg. to save the individuals' lives);
- Processing is carried out in the course of legitimate activities relating to a political, philosophical, religious or trade union aim, and with appropriate safeguards;
- The data subject has already 'manifestly' made the data public (ie. deliberately and obviously);
- Processing is necessary for the establishment, exercise or defence of legal claims, or by the courts;
- Processing is necessary for and proportionate to a 'substantial public interest' (as defined under local EU Member State laws);

1 https://www.bbc.co.uk/news/technology-48276660
2 https://www.bbc.co.uk/news/technology-49489154
3 https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position
4 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/
5 WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust, dated 19.02.20
6 Article 9(1) GDPR

- Processing is necessary for medical reasons;
- Processing is necessary for reasons of public health;
- Processing is necessary for archiving purposes in the public interest, and is proportionate.[7]

The meaning of *'for the purposes of uniquely identifying a natural person'* has been the subject of some debate. The judges in the recent case of R (Bridges) v Chief Constable of the South Wales Police relied on guidance stating that *"the notion of "identifiable" refers not only to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others"*.[8]

For example, the use of facial recognition techniques to monitor how frequently particular individuals fly would be caught by the rules: this would involve uniquely identifying specific travellers. On the other hand, merely scanning faces in an airport lounge for general physical characteristics and categorising a group of travellers according to gender or age-bracket would not fall within the 'special category' personal data governed by Article 9.[9]

For commercial operators wishing to use facial recognition technology in a way which triggers Article 9, explicit consent from data subjects is likely to be required. The app 'Clearview AI' is currently facing a lawsuit in the United States for 'scraping' images of millions of people from social media sites, gathering billions of pictures without their consent, and using these to form a database against which live photos can be compared for facial recognition purposes.[10]

Public bodies

Facial recognition technology is also increasingly being used by public bodies, notably for policing.[11] This was the subject of an ICO investigation that concluded in October 2019, and of the Bridges case referred to above. The Live Facial Recognition ("LFR") technology employed by the South Wales Police Forces involved the compilation of a watch-list of potential suspects, and the attribution of a 'biometric template' to each of these. The faces of members of the public were then scanned through video footage, a biometric template created of every individual's face, and this compared to the templates on the watch-list. If a match was found, then further action may have been taken. The biometric templates created of all other members of the public were instantly deleted.[12] The processing of personal data by the police in the UK is covered by Part 3 of the DPA 2018. The judges and the ICO ultimately concluded that the South Wales Police had acted lawfully towards Mr Bridges, and that no further regulatory action was needed. However, the ICO commented that more could be done to achieve higher standards of data protection compliance, and to improve public awareness and confidence in the technology.

Potential for discrimination

One key area highlighted by the ICO, and raised more widely in arguments against facial recognition, is the risk of technological bias. This could lead to discriminatory practices and imperfect data.[13] While the Court found no evidence of any discrimination in the use of technology employed by the South Wales Police, a recent study of the facial recognition technology developed by Microsoft, IBM and Face ++ (which combines facial recognition and artificial intelligence software) found that these misidentified 1% of lighter skinned males in a set of 385 photos, compared to 35% of darker skinned women in a set of 271 photos.[14] This could be the result of the under-representation of women and people of colour in the test data on which the technology is trained, meaning that it is less able to discern the differences between different faces.[15] If the use of such technology is to become widespread, every effort should be made to train the software fully, to ensure that it does not inadvertently lead to discriminatory practices.

CCTV

Use of CCTV cameras generally can involve the use of biometric data for identification purposes, especially when paired with biometric identification technology. The definition of 'biometric' personal data is broad, and may be interpreted differently in different EEA Member States. As for all personal data processing, when using CCTV organisations must tell the individuals concerned (by displaying clearly visible signs), ensure that they have a lawful basis for using it and control access to the footage. In the UK, organisations are also required to inform the ICO if using CCTV cameras, to explain why and to pay a data protection fee.

All organisations which process personal data in connection with the UK should consider whether they need to inform the ICO and pay the ICO's data protection fee. Use of CCTV cameras in the UK is one of the types of processing for which a fee is likely to be required. To find out more please visit the ICO website https://ico.org.uk/for-organisations/data-protection-fee/, or seek advice.

Action points

Organisations wishing to make use of CCTV and/or biometric identification techniques such as facial recognition should:

---

7 Article 9(2) GDPR

8 R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341 (Admin), paragraph 132, quoting the Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, at paragraph 18.

9 The data collected in the latter case, however, might still be personal data and subject to the standard rules under Article 6 of the GDPR.

10 http://www.pdp-email.com/compliance28012020/

11 In London, for example, the Metropolitan Police announced in January 2020 that they would be rolling out its use in targeted public spaces across the capital for certain, limited, periods of time: https://www.bbc.co.uk/news/uk-51237665

12 In line with the requirement in s.39(1) DPA 2018 that it be "Kept no longer than is necessary for the purpose for which it is processed". In the case of the South Wales Police it is deleted instantly - R (Bridges) v Chief Constable of the South Wales Police, para 16, and ICO report, pages 12 and 29

13 https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf, p34

14 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

15 https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf, p33

- Conduct thorough risk assessments to analyse the impact on the individuals involved;
- Consider which laws will apply: where will the individuals be located? Where will the technology be used?
- Inform the relevant data protection regulator(s) and pay any relevant fee to the regulator(s).
- Take advice where necessary.

Facial recognition technology, if used correctly, could be a valuable tool for both the private and public sectors. However, for the moment concerns remain about its reliability and the potential impact on the public's privacy. Make sure that you keep on the right side of the law, and avoid losing face.

For more information please contact

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

FELICITY BURLING
Associate, London
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

or your usual HFW contact.

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, competition and regulatory trade capabilities, please visit hfw.com/EU-Competition-and-Regulatory

hfw.com

Americas | Europe | Middle East | Asia Pacific