Press release: Metropolitan Police's use of Facial Recognition Technology at the Notting Hill Carnival, 2017

Paul Wiles, Biometrics Commissioner writes about the use of Facial Recognition Technology at the Notting Hill Carnival.

This kind of biometric technology (Facial Recognition Technology) has the potential to be a really useful crime fighting tool but we are not there yet. It needs to be properly tested and evaluated if it is going to be effective and it will need to be handled carefully by the police and the government if it is going to be trusted by the public.

Key messages

1. There is a public benefit in the use of such technology if it can be shown to help prevent the problems that there have been at previous carnivals by assisting the police to catch offenders or prevent crime.

2. Tests of facial matching for spotting individuals in large crowds have so far had very poor success – hence the Metropolitan Police's trial. It is good that they have made their trial public but they must carry out a proper evaluation and publish the results.

3. The police already hold over 20 million facial images but there is as yet no single, shared policing system for storing and searching police held images nor an evaluation of its accuracy and usefulness.

4. Police forces need to work together to agree on a single facial recognition system that has been proved to work in the field and government needs to create a legislative framework for its use, with independent oversight to provide public assurance, as it has done for DNA and fingerprints.

5. The previous Biometrics Commissioner made similar points as have others, such as the Science and Technology Select Committee, and we have yet to see what the government proposes as their Biometrics Strategy has been delayed for some time.

Broader explanation

1. Police already hold over 20 million facial images on both the Police National Database and in separate force systems. Her Majesty's Inspector of Constabulary (Scotland) recently commented unfavourably on this situation since it means that different standards are being applied across the UK. Most of these facial images are custody images. The courts held in 2012 that these holdings were unlawful and the Home Office responded to that judgment in 2017. I have commented on this response elsewhere.

2. Current police interest in facial matching has moved on from custody images to whether it can be used to identify individual offenders in public places. The capability to do this is still unproven since tests in such situations have shown very poor match rates unlike match rates in controlled environments.[1]

3. The police are conducting a number of trials to see if facial searching and matching technology can be employed effectively in crowded public places. Such experiments should be properly designed and evaluated, preferably involving external experts, and the results published. The police should also evaluate their use of facial images generally in order to demonstrate that they have a useful and cost-effective purpose, based on adequate matching quality. They also need to explain how they will deal with potential false matches.

4. There is limited research on this area and most of it has been conducted in the USA. Evaluations should include not just the behaviour of the matching algorithms but how they work in the total criminal justice system and how human decision making in such systems affects the accuracy of match rates.[2]

5. Facial matching systems have improved significantly recently and the use being explored by the Metropolitan Police may, at some point, reach acceptable quality for operational use but presently that remains to be demonstrated.

6. The use of facial images, especially in public places, is very intrusive of individual freedom, especially because images can be captured without the subject being aware. The public benefit of the use of such an intrusive technology must outweigh the interference in individual privacy. Such a difficult balance between public benefit and individual privacy should not be decided by the police but is best decided by Parliament through informed debate and legislation. As is currently the case for DNA and fingerprints the legislation should include independent oversight to reassure the public that their privacy is being properly

protected.

Paul Wiles, Biometrics Commissioner

[1] The most extensive evaluations of the facial matching capabilities of different systems have been carried out by the US National Institute of Standards and Technology (NIST).

[2] See e.g. D. White et al: Error Rates in Users of Automatic Facial Recognition Software, Plos One, 2015, 10 (10): eo 139827, showing how human error can reduce further the effectiveness of facial recognition systems.