Press release: Response to the Home Office review of the retention and use of custody images

The use of facial images has been a regular part of policing since the development of photography led to the taking of custody images. The current use of facial images is different in that images are now digital, can be housed on a national database and searched using software based on algorithms that claim to find possible matches.

The use of such images is important in policing and it is in the public interest that they are used to prevent, detect or prosecute crime. However, because capturing, storing and searching such images is intrusive of individual privacy there is a need to ensure that the use of facial images is within a governance framework that strikes an acceptable and proportionate balance between public benefit and individual privacy.

In 2012 the High Court held that the governance framework then used by the police was not proportionate in its retention rules and as such was unlawful. The court drew attention to the 'risk of stigmatisation of those entitled to the presumption of innocence' and that holding images of those unconvicted for a long period (a minimum of 6 years) was not proportionate. They added that retaining images in such cases for minors would be especially harmful.

The recently published Home Office review of the use and retention of custody images makes proposals as to a future governance of the police use of facial images in order to make their use more proportionate in response to the Court's ruling.

The review still proposes that a routine police review of retention of those who should be presumed innocent should happen only after 6 clear years for a Group 3 offence and 10 clear years for Group 1 or 2 offences. The only response to the Court judgment is that such individuals may apply to the police to have their images deleted after the conclusion of proceedings. In considering such applications there should be a 'presumption in favour of deletion' and a 'strong presumption' in the case of those under 18 but that the police are entitled to refuse such an application.

Adding this limited application process does add a degree of proportionality but whether this would be enough in the face of any future challenge may depend on how many presumed innocent people apply successfully to have their images deleted before the minimum 6 year review period. The nearest equivalent existing process is that of the records deletion process whereby people can apply to the police to have their arrest records and/or biometric records deleted from the Police National Computer.

In the year ending on 31 March 2016, Home Office statistics show that 896,209 people were arrested for a notifiable offence and in the same period 1,003

applied to have their police records deleted, of which 233 were accepted by the police.

The review leaves the governance and decision making of this new process entirely in the hands of the police but future public confidence might require a greater degree of independent oversight, transparency and assurance than is proposed.

The applications process, the power to nevertheless retain and the routine reviews mean that the compliance costs of this proposal will be high because individual decisions will have to be made in every case. Although the review proposes that guidance should be issued about making such decisions there still might be variation in decision making between forces resulting in a postcode lottery as to whether images are retained.

In addition, deletion will happen some time after the police decide to take no further action against a subject and it is not clear how far legacy holdings will be weeded against these proposed new retention rules. If there is a ‘presumption of deletion’ then these costs could all be avoided and the process made more timely by automatic deletion. This could be built into Police National Database and the next generation of databases currently being developed.

The review suggests that the retention and use of facial images is ‘generally less intrusive (than DNA or fingerprints) as many people’s faces are on public display all the time’. I disagree with that assertion. In fact for that reason the use of facial images is more intrusive because image capture can be done using cameras in public places and searched against government databases without the subject being aware. Facial images are no longer only used solely for custody purposes and image capture and facial searching capabilities have and are being used by the police in public places.

The review points out that the police are currently using a number of different databases and matching software products. The Police National Database currently holds 19 million images and that does not include all police forces and most notably the images held on a separate database by the largest police force, the Metropolitan Police Service. The review provides no statistical information in relation to how these databases are being used or to what effect.

The fact that so many different systems are in use means that the software used is of varying quality and the consequent processes of interpretation will also vary. In spite of that the review encourages all forces to pool their images in the existing national national. As a recent report by HMIC(S) concluded: ‘This means that differing standards are being applied to a common UK database’.

Use of facial image database searching for intelligence purposes requires that users understand the scientific quality and reliability of the software and use a common process of interpretation and assessment that takes account of any weaknesses or biases in the overall system. To achieve this, the police need to move to a common database, matching software and interpretive

process which can provide the best available quality and reliability and is understood by all those using the system. Such a new system ought to meet quality standards set by the Forensic Science Regulator.

Furthermore, since the review envisages future facial images database information being available to the rest of the criminal justice system then such a system needs to be totally transparent in its mode of operation if it is to meet evidential requirements.

My predecessor made similar comments about the problems with the current police use and retention of facial images.

Paul Wiles Biometrics Commissioner