



Home Office

Review of the Use and Retention of Custody Images

February 2017



© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gsi.gov.uk

Contents

1. Executive Summary	1
2. The Revised Retention Regime	9
Under 18s.....	12
(a) <i>Unconvicted individuals whose image was taken when they were under 18</i>	12
(b) <i>Individuals convicted of a recordable offence whose image was taken when they were under 18</i>	13
(c) <i>Individuals convicted of a non-recordable offence whose image was taken when they were under 18</i>	14
3. Consideration of the issues	15
Capture and quality assurance of custody images.....	15
Police use and management of custody images.....	15
<i>Adults without criminal convictions</i>	15
<i>Deletion of the images of convicted individuals</i>	16
Custody images and PND	16
Future systems.....	17
Other considerations	17
4. Background	19
5. The current legal and operational framework	20
6. The use and administration of custody images	22
Capture and quality assurance of custody images.....	22
Police use and management of custody images.....	22
Custody images and PND	23
Other jurisdictions' retention of custody images.....	26
Annex A: Review of legal base, regulation, governance and procedures for the use and retention of custody images	27
Terms of reference	27
<i>Issue</i>	27
<i>Objective</i>	27
<i>Scope</i>	27
<i>Product</i>	28
Annex B: Methodology for the custody image review	29
Annex C: Governance of PND	30
Annex D: Review of published information relating to the civil liberties/privacy implications of the retention and use of custody images	31
Privacy and civil liberties	31

Human ability to recognise individuals from images.....	33
References	36

1. Executive Summary

1.1 In 2012, the High Court ruled, in the case of *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)¹ ('RMC'), that the retention of images from unconvicted individuals² under the Metropolitan Police Service's policy for the retention of custody images, which followed the Code of Practice on the Management of Police Information and accompanying guidance ('MoPI'), was unlawful. In response to this judgment, the Government commissioned a review of the current framework for the acquisition, retention and deletion of custody images³ as well as their operational uses and governance arrangements (the Custody Image Review). The review is designed to advise Ministers on:

- the current legal and operational framework, including relevant guidance on procedures, and whether they adequately address relevant case law developments in relation to the right to respect for private and family life as set out in Article 8 of the European Convention on Human Rights ('ECHR');
- the utility and benefits of custody images in meeting policing purposes and expected future developments in their use, including automated facial searching, and;
- options for change where this appears necessary in relation to regulation, governance, oversight, policies and guidance.

The terms of reference of this review are set out at Annex A and the methodology is set out at Annex B.

1.2 Section 64A of the Police and Criminal Evidence Act 1984 ('PACE') provides police with the power to take facial photographs (known as 'custody images') of anyone who is detained following arrest⁴. The regime⁵ governing the retention of custody images is set out in the Code of Practice on the Management of Police Information 2005 ('MoPI') and guidance contained in the College of Policing's Authorised Professional Practice on Retention, Review and Disposal ('the APP'), although this was developed for all information held by the police and does not provide specific guidance in respect of custody images.

1.3 Custody images are a standard feature of everyday policing. The most common use of such images is to brief frontline officers so that they can identify suspects, offenders and those on bail. Custody images are also used in investigations, for witness identification, and to assist with searching for unidentified suspects.

1.4 The total numbers of images stored by the forces that participated in this Review ranged from 26,816 in the smallest of the eight forces, to 7.8 million in the largest⁶. A range of local custody systems, such as Niche, National Strategy for Police Information Systems ('NSPIS'), and Athena as well as bespoke force systems, are used to store the images. These systems are generally not linked to Crown Prosecution Service ('CPS') or court

¹ <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf>

² This review uses the term 'unconvicted individuals' to refer collectively to individuals who have not been convicted of (or cautioned for) any offence.

³ Custody images are taken under S64A of the Police and Criminal Evidence Act 1984 (PACE). The scope of this review expressly excludes images which were primarily gathered as intelligence and/or are held as evidence. This is because such images are held as police information or evidence in relation to specific events, rather than for verifying the identity of an individual who is already known to the police.

⁴ Separate considerations apply in relation to individuals arrested under an extradition arrest power.

⁵ Referred herein collectively as 'the MoPI regime'

⁶ As at March 2015.

systems. They are not generally designed to automatically weed, review or destroy images, or to differentiate between convicted and unconvicted individuals although the Athena system (currently used by seven forces) can allow images to be retained and deleted in accordance with pre-set criteria (such as the length of time retained) if this capability is enabled by individual forces.

- 1.5 The police's ability to make use of custody images is enhanced by their ability to upload them from forces' local custody IT systems onto the Police National Database ('PND'), which has been in place since 2010. Now all but nine forces upload custody images onto PND. As of July 2016, there were over 19 million custody images on PND, over 16 million of which had been enrolled in the facial recognition gallery making them searchable using facial recognition software. Many of these images are multiple images of the same individual. Recent advances in technology mean that it is now possible to search custody images on PND.
- 1.6 Before uploading a custody image to PND, forces should first check, in line with the APP⁷, whether it provides useful intelligence to the force. For example, where up-to-date images of the individual already exist, it may be unnecessary to retain a further image.
- 1.7 In broad terms, this review proposes giving individuals the facility (if they have not been convicted⁸ of the offence(s) in relation to which the custody image was taken (whether or not it is recordable⁹) to apply to chief officers of police forces to have their custody image deleted. This is similar to the approach of some other European jurisdictions such as Belgium and the Netherlands (see paragraph 6.19). Where such an application is made it is recommended that there should be a presumption in favour of deletion, with chief officers having the discretion to retain an image where this is necessary for a policing purpose and there is an exceptional reason to do so. This review sets out what factors might be taken into consideration when such applications are made. Where the images of unconvicted individuals are not deleted, or where no application is received, this review recommends that they should be reviewed in accordance with scheduled review periods set out in the APP, with a presumption of deletion at the first scheduled review, unless there is an exceptional reason to retain the image.
- 1.8 There should be an even stronger presumption of deletion upon application for unconvicted individuals whose image was taken when they were under 18 years old i.e. retention only where there is a highly exceptional reason to do so. In addition, there should be a presumption that images taken of people when they were under 18 are deleted at the first APP review.
- 1.9 Those convicted of recordable offences should also have a right to apply for the deletion of their custody image. However, there would be no presumption of deletion in such cases. Such individuals would only be able to apply for deletion six or ten years after conviction (or six or ten years after their release from custody if sentenced to a term of imprisonment or detention regardless of whether the image was taken in relation to the

⁷ <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#deciding-to-retain>

⁸ For the purposes of this review, a 'conviction' includes a caution, warning, reprimand, finding of not guilty by reason of insanity or a finding that an individual is under a disability but has done the act charged as set out in section 65B of the Police and Criminal Evidence Act 1984 ('PACE'). Additionally, the reference to 'convicted' individuals or youths means someone who is convicted of (or cautioned, warned, reprimanded etc. for) any recordable offence in relation to which the custody image under consideration was taken.

⁹ Recordable offences are listed in the National Police Records (Recordable Offences) Regulations 2000 pursuant to section 27 of PACE which means that the police are permitted to keep a record (for example on the Police National Computer) of the offence. Generally speaking, they are imprisonable; however, it also includes a number of non-imprisonable offences set out by the Schedule to the Regulations.

offence for which they are in custody) depending on the nature of the offence. Where no request for deletion is made by a convicted individual, this review recommends that the retention of their custody image should be reviewed in accordance with the time periods for scheduled reviews contained in the APP and we have set out specific factors that might be taken into account when such a review is undertaken.

- 1.10 Convicted individuals whose image was taken when they were under 18 should also have a right to request the deletion of their custody image. They would be allowed to apply for deletion six or ten years after conviction (or six or ten years after release from custody if sentenced to a term of imprisonment or detention regardless of whether the image was taken in relation to the offence for which they are in custody) depending on the seriousness of the offence. Where such an application is made, it is recommended that there should be a presumption in favour of deletion, with chief officers having the discretion to retain an image where this is necessary for a policing purpose and there is an exceptional reason to do so.
- 1.11 Although non-recordable offences are generally considered to be less serious than recordable ones, nevertheless this review makes a distinction between individuals convicted of such offences and those who are unconvicted. As with Group 3 recordable offences, an individual convicted of a non-recordable offence will have to wait six years before applying for the deletion of their custody image and forces will be required to carry out a scheduled review six clear years after conviction and every five clear years thereafter if the image is retained. However, unlike with Group 3 recordable offences, there will be a presumption in favour of deletion of the image both when the individual applies and when a scheduled review takes place.
- 1.12 For the avoidance of any doubt, the concept of clear periods¹⁰ will apply in determining the timing of all scheduled reviews of the retention of custody images. A clear period is defined by the APP as “the length of time since an individual last came to the attention of the police as an offender or suspected offender for behaviour that can be considered a relevant risk factor”¹¹. In practice, this means that the timing of a scheduled review depends on the individual not coming to the attention of the police as an offender or suspected offender for a ‘clear’ number of years after they are convicted, acquitted or a decision is made to take no further action against them. If they do come to the attention of the police in the interim, then the time period between scheduled reviews would be reset until the relevant clear period is completed. However, clear periods will not apply in determining when forces are required to consider a request for the deletion of a custody image or images from a convicted or unconvicted individual.
- 1.13 This approach balances the need to use information, data and intelligence to protect the public, against the Article 8 rights of individuals. It also takes account of the high estimated cost to the taxpayer of a full manual deletion exercise in respect of all custody images currently held.
- 1.14 It is expected that the implementation of any new technological solutions, both local and national, will link and integrate intelligence, crime and prosecution data providing a better ability to search, access and assess custody images leading to improved risk-based retention and deletion.

¹⁰ A clear period is defined by the APP as ‘the length of time since a person last came to the attention of the police as an offender or suspected offender for behaviour that can be considered a relevant risk factor’.

¹¹ <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#clear-periods>

1.15 We have considered whether there would be a benefit in applying a regime similar to the one that operates for fingerprints and DNA, as set out in PACE as amended by the Protection of Freedoms Act 2012 ('PoFA'). However, we have decided against introducing such a regime for a number of reasons:

- the law on custody images under PACE¹² is quite distinct from that on DNA and fingerprints;
- unlike DNA and fingerprints, facial images are generally less intrusive as many people's faces are on public display all of the time;
- custody images are used in different ways to DNA and fingerprints (for example, in identity parades and for briefing front-line officers);
- unlike DNA and fingerprints, the usefulness of a custody image declines over time, especially in respect of younger people; and
- each force would need to carry out a manual weeding of their custody images which would be expensive and time consuming.

1.16 This review therefore makes the following recommendations¹³:

Recommendation 1

APP guidance should be updated to set out the specific considerations for the retention of custody images which are outlined in this review. Guidance should be clear that police forces must continue to act in accordance with all relevant legislation, in particular the Data Protection Act 1998 ('the DPA'), the European Convention on Human Rights ('ECHR'), and the Equality Act 2010. Records which no longer have a policing purpose should be archived for long-term retention outside the operational environment if this is required by law, for example under the Inquiries Rules 2006 made under the Inquiries Act 2005¹⁴; it must be clear that the records are kept for this discrete purpose only. Further, notwithstanding the recommendations made below, custody images may be retained where the individual concerned has given informed written consent to this (which may also be withdrawn, in writing, at any time).¹⁵

Recommendation 2

Whenever consideration is given to the retention of a custody image, whether on application or otherwise, regard should be had to the quality of the image (including resolution, size etc.) as well as to how accurately it identifies the individual concerned (i.e. having regard to any changes in appearance), and therefore its utility in identification (including facial searching) on the Police National Database ('PND').

Recommendation 3

For the avoidance of any doubt, the concept of clear periods should apply in determining the timing of all scheduled reviews of the retention of custody images. However, clear periods should not apply in determining when forces are required to consider a request for the deletion of a custody image or images by a convicted or unconvicted individual.

¹² Section 64A.

¹³ The recommendations in this review apply to images currently retained by the police as well as those retained in the future.

¹⁴ http://www.legislation.gov.uk/uksi/2006/1838/pdfs/ukxi_20061838_en.pdf

¹⁵ Where appropriate, for example where someone is incapable of giving or withdrawing consent in their own right, this may be done on their behalf.

Recommendation 4

Individuals should be able to apply to have their custody image deleted according to the timetable set out in Table 1 below.

Table 1: Individual applying for the deletion of a custody image

Situation	When can an individual apply for their custody image to be deleted?
Any age convicted of a Group ¹⁶ 1 or 2 offence	<p>Ten years after conviction (or release from custody if sentenced to a term of imprisonment or detention). A suspended sentence should be treated in the same way as an immediate term of imprisonment.</p> <p>If an application for deletion is refused then individuals may apply again for deletion after a further ten years have elapsed.</p>
Any age convicted of a Group 3 recordable offence.	<p>Six years after conviction (or release from custody if sentenced to a term of imprisonment or detention). A suspended sentence should be treated in the same way as an immediate term of imprisonment.</p> <p>If an application for deletion is refused then individuals may apply again for deletion after a further five years have elapsed.</p>
Any age convicted of a non-recordable offence	<p>Six years after conviction.</p> <p>If an application for deletion is refused then individuals may reapply after a further five years have elapsed.</p>
Any age arrested for, but not convicted of, any offence whether recordable or non-recordable	<p>After the conclusion of proceedings¹⁷</p> <p>If an application for deletion is refused then individuals reapply once the next relevant scheduled review period has been carried out or after 12 months (whichever is sooner).</p>

¹⁶ The APP splits offences into four different categories: Group 1 – these are offences concerning public protection issues; Group 2 – other sexual, violent or serious offences, Group 3 – All other offences and Group 4 - information on undetected crime, intelligence products, missing persons, and victims and witnesses. This review concerns itself with Groups 1, 2 & 3 only.

¹⁷ For example, after they are informed that they will not be prosecuted for, or charged with the offence, where they are charged but the case discontinued, where they are acquitted in court or where the conviction is quashed on appeal etc..

Recommendation 5

Police forces should adopt the regime in Table 2 on receipt of a request for a custody image to be deleted.

Table 2: Police action on receipt of a request for deletion of a custody image¹⁸

Applicant	Presumption of deletion
Adult convicted of a recordable offence	No presumption in favour of deletion
Adult convicted of a non-recordable offence	Presumption in favour of deletion
Adult arrested for, but not convicted of, an offence	
Under 18 convicted of a recordable offence	
Under 18 convicted of a non-recordable offence	Strong presumption in favour of deletion
Under 18 arrested for, but not convicted of, an offence	

¹⁸ Assumes request is made within timeframes set out in Table 1.

Recommendation 6

Police forces should adopt the regime in Table 3 in relation to the review of custody image for which no application for deletion has been made.

Table 3: Scheduled reviews by the police of custody images – no request from individual

Situation	Timeframe for Police action	Presumption for the Police as part of review process
Adult convicted of a Group 1 or 2 offence	Every ten clear years after date of conviction (or release from custody if sentenced to a term of imprisonment).	No presumption in favour of deletion
Adult convicted of a Group 3 recordable offence	Six clear years after date of conviction (or release from custody if sentenced to a term of imprisonment), then every five clear years.	
Adult convicted of a non-recordable offence	Six clear years after conviction, then every five clear years.	Presumption in favour of deletion
Adult arrested for, but not convicted of, a Group 1 or 2 offence	Every ten clear years from date of conclusion of proceedings.	
Adult arrested for, but not convicted of, a Group 3 offence	Six clear years from date of conclusion of proceedings, then every five clear years.	
Under 18 convicted of a Group 1 or 2 offence	Every ten clear years after date of conviction (or release from custody if sentenced to a term of imprisonment or detention).	
Under 18 convicted of a Group 3 recordable offence	Six clear years after date of conviction (or release from custody if sentenced to a term of imprisonment or detention), then every five clear years.	
Under 18 convicted of a non-recordable offence	Six clear years after date of conviction (or release from custody if sentenced to a term of imprisonment or detention), then every five clear years.	
Under 18 arrested for, but not convicted of, a Group 1 or 2 offence	Every ten clear years from date of conclusion of proceedings.	Strong presumption in favour of deletion
Under 18 arrested for, but not convicted of, a Group 3 offence	Six clear years from date of conclusion of proceedings, then every five clear years.	

Recommendation 7

Chief Officers must ensure that national standards on custody image collection are adhered to.

Recommendation 8

Police forces should continue to have discretion to delete the images of both convicted and unconvicted individuals, as is currently the case under the APP.

Recommendation 9

As part of their review of MoPI compliance, chief officers must ensure that they can confidently say whether or not they hold an image of a specific individual and that they consider deletion applications by individuals according to the new retention regime.

Recommendation 10

The APP Guidance should be updated to take account of the review's recommendations on the retention of custody images.

Recommendation 11

Forces must ensure that they are processing custody images in compliance with the provisions of the Data Protection Act 1998 and other relevant legislation.

Recommendation 12

Future local or national IT systems, that will be used for the storage of images, should be designed to integrate relevant data – including court and CPS data – to facilitate a more efficient method of search, retrieval and deletion of images and aim to link and integrate intelligence, crime and prosecution data (subject to relevant legal considerations), and that this should be regularly reviewed.

Recommendation 13

The use of PND should be further promoted through the National Police Chiefs' Council ('NPCC') lead. The NPCC lead should ascertain the future plans of the nine forces who are not uploading custody images to PND.

Recommendation 14

The independent Digital Ethics Panel for Policing, in conjunction with the DNA Ethics Group, should consider how they can work together to address the ethical issues relating to the use of custody images.

Recommendation 15

The custody image retention regime should be reviewed again in 2020.

2. The Revised Retention Regime

2.1 The recommendations in this review bring in a new regime for the retention of custody images from both convicted and unconvicted individuals. Further detail on the recommendations is set out below.

Adults

(a) Unconvicted individuals

2.2 Chief officers should be required to consider the deletion of a custody image, following an application in writing for its destruction by the individual (or, where the individual is incapable of applying themselves, an application made on their behalf), provided that the individual has not been convicted of the offence(s) in relation to which the custody image was taken.

2.3 Any such application would only be considered after investigations in relation to the offence(s) in relation to which the image was taken have concluded and no charges have been brought, or charges have been brought but the Crown Prosecution Service ('CPS') decided not to prosecute, or the individual was prosecuted but acquitted¹⁹ (and no appeal is pending), or after a successful appeal. Where an application is made by an individual who is subject to another active investigation(s), for which a separate image(s) exists, then this policy is not intended to prevent the retention of that image (unless and until the other investigation or proceedings come to an end and a separate application is made in relation to that image).

2.4 There should be a presumption that custody images of unconvicted individuals are deleted following such an application. However, chief officers should have the discretion to retain an image where this is necessary for a policing purpose (as specified by paragraph 2.2.2 of the Code of Practice on the Management of Police Information ('MoPI')) and there is an exceptional reason to do so, which may include one or more of the following (this list is not meant to be exhaustive):

- an assessment using the National Risk Assessment Criteria ('NRAC') suggests that the individual is likely to pose a substantial risk of harm;
- there is intelligence or evidence to suggest that an individual may be dangerous, for example they are entered on the Violent and Sex Offender Register ('VISOR') system as a 'Potentially Dangerous Person';
- there are still active investigations in which that individual is a suspect;
- the individual has known links to organised crime or terrorism;
- the image is needed, or is likely to be needed, to enforce a civil order (such as orders which may be imposed under the Anti Social Behaviour Crime and Policing Act 2014).

2.5 An application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal which sets out the reasons for refusing the application (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). In the latter case, the notification should state when the retention will next be subject to a scheduled review, and explain that the individual may apply again for deletion once that scheduled review period has passed or after 12 months (whichever is sooner). The concept of clear

¹⁹ If an individual is acquitted of some, but not of all, of the offences in relation to which the custody image under consideration was taken then they will be treated as a convicted individual.

periods will apply in determining the timing of the scheduled review but it will not apply in determining when a force is obliged to consider the first and subsequent application from an unconvicted individual for the deletion of their custody image.

2.6 Where images of unconvicted people are retained (either because no application for deletion has been received or where this has been refused) then they should be reviewed in accordance with the scheduled review periods set out in the APP guidance. This includes the application of the policy on clear periods for all offences. This means that a scheduled review should take place six (for Group 3) or ten (for Group 1 and 2 offences) clear years after the date of acquittal or decision to taken no further action ('NFA'), and then every five (Group 3) or ten (Groups 1 and 2) clear years thereafter (unless a force has opted to automatically delete them after a specified time-period as specified in the APP)²⁰²¹. For a summary of the review framework, see tables 2 & 3.

2.7 Even where no application for deletion has been received, there should be a presumption that images of an individual who has not been convicted are deleted at the first scheduled review, unless retention is necessary for a policing purpose (as specified by paragraph 2.2.2 of MoPI) and there is an exceptional reason to do so, which may include the factors outlined at paragraph 2.7 above (i.e. the same test that chief officers need to apply upon an application to delete).

2.8 As set out in the APP, such images should also be the subject of an initial review and evaluation and, where appropriate, triggered reviews. Where the appropriate APP reviews have not taken place for images currently held then this must be done as soon as is reasonably practicable.

(b) Convicted of a recordable offence

2.9 Images of individuals convicted of a recordable offence should be scheduled for review in accordance with the time periods currently set out in the APP. This includes the application of the policy on clear periods for all categories of offences. This means that a scheduled review should take place six (for Group 3) or ten (for Group 1 and 2 offences) clear years after the date of sentence (or release from custody if sentenced to a term of imprisonment), and then every five (Group 3) or ten (Groups 1 and 2 offences) clear years thereafter (unless a force has opted to automatically delete them after a specified time-period as specified in the APP). For a summary of the review framework, see tables 2 & 3.

2.10 When such reviews take place, chief officers will need to consider whether retention of the image is necessary for a policing purpose (as specified by paragraph 2.2.2 of MoPI) and proportionate to the level and type of risk an individual poses. However, there will be no presumption in favour of deletion in such cases. The factors to consider in making this assessment might include one or more of the following (this list is not meant to be exhaustive):

- an assessment using NRAC suggests that the individual is likely to pose a substantial risk of harm;
- there is intelligence or evidence to suggest that an individual may be dangerous, for example they are entered on the VISOR system as a 'Potentially Dangerous Person';

²⁰ <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/#group-3-all-other-offences>

²¹ Where an individual's custody image is taken in relation to multiple offences, then the most serious offence determines the APP category.

- there are still active investigations in which that individual is a suspect;
- the seriousness of the offence for which the individual was convicted in relation to other offences in the same APP group;
- the individual has known links to organised crime or terrorism;
- the image is needed, or is likely to be needed, to enforce a civil order (such as orders which may be imposed under the Anti Social Behaviour Crime and Policing Act 2014).

2.11 A convicted individual, whose custody image is retained, may apply for its deletion but only after the minimum period of six years (Group 3) or ten years (Group 1 or 2) has passed since they were convicted (or released from custody if sentenced to a term of imprisonment). In contrast to the unconvicted (and those convicted of non-recordable offences), there should be no presumption of deletion when a review takes place. In coming to a decision on retention, any relevant factors set out under paragraph 2.10 above should be taken into consideration.

2.12 As with unconvicted individuals, an application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal, which states the reasons why the application has been refused (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). The notification should set out when an individual may make a new application for deletion; five years in the case of Group 3 and ten years in the case of Group 1 or 2 offences. The concept of clear periods will apply in determining the timing of the scheduled review but not in determining when a force is obliged to consider the first and subsequent application from a convicted individual for the deletion of their custody image.

2.13 Whilst an individual is in prison, this review recommends that individuals are not permitted to apply for the deletion of their custody image. This is because we consider a term of imprisonment to be so serious that the police are almost certain to refuse such an application. Therefore, in order to avoid unnecessary work for the police, the six (for Group 3) or ten (for Groups 1 or 2) year period after which deletion will only begin upon their release. Where an individual who is released from custody receives a further term of imprisonment before the six or ten year period has expired, the 'clock' will be reset and will start again upon their second release. Suspended sentences will be treated in the same manner as immediate sentences of imprisonment.

(c) Convicted of a non-recordable offence

2.14 As with those convicted of a Group 3 offence, individuals convicted of non-recordable offence may apply for the deletion of their image after a period of six years. Scheduled reviews for such images should take place six clear years after conviction then (if the image is retained) every five clear years. Unlike recordable offences, there shall be a presumption in favour of deletion; both where an application is made and when a scheduled review takes place. In coming to a decision, the factors set out at paragraph 2.10 should be taken into consideration, insofar as they are relevant.

2.15 An application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal, which states the reasons why the application has been refused (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). The notification should set out when an individual may make a new application for deletion; five years in the case of Group 3 and ten years in the case of Group 1 or 2 offences. The concept of clear periods will apply in determining the timing

of the scheduled review but not in determining when a force is obliged to consider the first and subsequent application from a convicted individual for the deletion of their custody image.

Under 18s

(a) Unconvicted individuals whose image was taken when they were under 18²²

2.16 It is recommended that chief officers be required to consider the deletion of a custody image, following the application for its deletion by an individual whose images were taken when they were under 18 (or, where the individual is incapable of applying themselves, an application made on their behalf), provided that the individual has not been convicted of the offence(s) in relation to which the custody image concerned was taken. Such an application would only be considered after investigations in relation to the offence(s) in relation to which the image was taken have concluded, and no charges have been brought, or charges have been brought but the CPS decided not to prosecute, or the individual was prosecuted but acquitted (and no appeal is pending), or an appeal has been successful. Where an application is made by an individual who is subject to another active investigation(s), for which a separate image(s) exists, then this policy is not intended to prevent the retention of that image (unless and until the investigation/proceedings come to an end and a separate application is made in relation to that image). For the purposes of such an application, it does not matter whether or not the individual concerned is still aged under 18.

2.17 There should be a strong presumption that the image taken from an unconvicted under 18 is deleted following such an application. However, chief officers will have the discretion to retain an image where this is necessary for a policing purpose (specified in paragraph 2.2.2 of MoPI) and there is a highly exceptional reason to do so, which might include one or more of the following (this list is not meant to be exhaustive):

- an assessment using NRAC suggests that the individual is likely to pose a **very** substantial risk of harm;
- there is intelligence or evidence to suggest that an individual may be dangerous, for example they are entered on the VISOR system as a 'Potentially Dangerous Person';
- there are still active investigations in which that individual is a suspect;
- the individual has known links to organised crime or terrorism;
- the image is needed, or is likely to be needed, to enforce a civil order (such as orders which may be imposed under the Anti Social Behaviour Crime and Policing Act 2014).

2.18 An application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal which states the reason why the application has been refused (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). In the latter case, the notification should set out when the retention will next be reviewed, and that the individual may apply again for deletion once the relevant scheduled review period has passed or after 12 months (whichever is sooner). The concept of clear periods will apply in determining the timing of scheduled reviews, but, it will not apply in determining when a force is obliged to consider the first and any subsequent reapplication from an unconvicted individual for the deletion of their custody image.

²² Referred to collectively as “unconvicted under 18s”.

2.19 Where an unconvicted individual whose image was taken before they were 18 years old does not apply for its deletion, then the retention of the image should be reviewed in accordance with the scheduled review periods set out in the APP guidance. This includes the application of the policy on clear periods for all categories of offences. This means that a scheduled review should take place six (for Group 3 offences) or ten (for Group 1 or 2 offences) clear years after the date of acquittal or decision to taken no further action ('NFA'), and then every five (Group 3) or ten (Groups 1 and 2) clear years thereafter (unless a force has opted to delete them after a specified time-period, prior to the end of the first six or ten year clear period).²³ For a summary of the review framework, see tables 2 & 3.

2.20 Even where no application for deletion has been received, there should be a strong presumption that images of unconvicted under 18s are deleted at the first scheduled review, unless retention is necessary for a policing purpose (as specified by paragraph 2.2.2 of MoPI) and there is a highly exceptional reason to do so, which may include the factors outlined at paragraph 2.14 above (i.e. the same test that chief officers need to apply upon an application to delete).

(b) Individuals convicted of a recordable offence whose image was taken when they were under 18

2.21 Individuals whose image was taken when were under 18, who are convicted of any recordable offence in relation to which the image was taken, continue to be scheduled for review in accordance with the time periods specified in the APP. This means that a scheduled review should take place six (for Group 3 offences) or ten (for Group 1 or 2 offences) clear years after the date of sentence (or release from custody if sentenced to a term of detention), and then every five (Group 3 offences) or ten (Group 1 and 2 offences) clear years thereafter (unless a force has opted to delete them after a specified time-period, prior to the five year review period in respect of Group 3 offences. For a summary of the review framework, see tables 2 & 3

2.22 Unlike individuals whose image was taken when they were over 18, there should be a presumption in favour of deletion at the first APP review. However, chief officers should have the discretion to retain an image where this is necessary for a policing purpose (as specified in paragraph 2.2.2 of MoPI) and there is an exceptional reason to do so, which might include (this list is not meant to be exhaustive):

- an assessment using NRAC suggests that the individual is likely to pose a substantial risk of harm;
- there is intelligence or evidence to suggest that an individual may be dangerous, for example the individual is entered on the VISOR system as a 'Potentially Dangerous Person';
- there are still active investigations in which that individual is a suspect;
- the seriousness of the offence for which the individual was convicted in relation to other offences in the same APP group;
- the individual has known links to organised crime or terrorism;
- the image is needed, or is likely to be needed, to enforce a civil order (such as orders which may be imposed under the Anti Social Behaviour Crime and Policing Act 2014).

²³ Where an individual's custody image is taken in relation to multiple offences, then the most serious offence determines the APP category.

- 2.23 Convicted individuals, whose custody image was taken before they were 18 years old, may apply for the deletion of their image after the minimum period of six years (Group 3) or ten years (Group 1 or 2) offences has passed since they were convicted (or released from custody if sentenced to a term of detention). There should be a presumption in favour of deletion when a review takes place. In coming to a decision on retention, the factors set out under paragraph 2.20 above should be taken into consideration. Where a chief officer turns down a request to delete an image that was taken when the individual was under 18, the force is not obliged to consider any further requests for a further five years (Group 3) or ten years (Groups 1 or 2).
- 2.24 An application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal, which states the reasons why the application has been refused (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). The notification should set out when an individual may make a new application for deletion; five years in the case of Group 3 and ten years in the case of Group 1 or 2 offences. The concept of clear periods will apply in determining the timing of the scheduled review but not in determining when a force is obliged to consider the first and subsequent application from a convicted individual for the deletion of their custody image.

(c) Individuals convicted of a non-recordable offence whose image was taken when they were under 18

- 2.25 As with those convicted of a Group 3 offence, individuals convicted of non-recordable offence may apply for the deletion of their image after a period of six years. . A scheduled review of such images should take place six clear years after conviction then (if the image is retained) every five clear years. However, unlike with recordable offences, there shall be a strong presumption in favour of deletion, both where an application is made and for scheduled reviews. In coming to a decision on retention, the factors set out under paragraph 2.20 above should be taken into consideration.
- 2.26 An application to a chief officer should be answered either with a confirmation that the image will be deleted, or a notification of refusal, which states the reasons why the application has been refused (unless there are compelling policing reasons not to disclose the basis for refusal, for example where the individual is part of an ongoing investigation). The notification should set out when an individual may make a new application for deletion; five years in the case of Group 3 and ten years in the case of Group 1 or 2 offences. The concept of clear periods will apply in determining the timing of the scheduled review but not in determining when a force is obliged to consider the first and subsequent application from a convicted individual for the deletion of their custody image.

3. Consideration of the issues

Capture and quality assurance of custody images

3.1 Forces are generally compliant with national standards although there is some room for improvement. This review found variation of practice in how custody images are captured in forces. This means that the quality of images varies, which has an impact on the utility of images. **Chief officers must ensure that national standards on custody images are adhered to.**

Police use and management of custody images

3.2 We note that APP reviews apply to images as they do to all police information. However, whilst the MoPI regime provides a framework for the retention of all police information, it gives no specific consideration to custody images.

3.3 The police use custody images for a range of operational applications. The case studies in this review, along with others that have been brought to our attention throughout the review, highlight a number of situations where a custody image has been the only way of identifying an offender, eliminating an innocent individual or otherwise protecting the public. Therefore, whilst proper consideration must be given to the privacy of individuals, particularly the innocent, this needs to be balanced carefully against the need to protect the public more widely.

Adults without criminal convictions

3.4 A different approach to retention should apply to convicted people and those without a criminal conviction. Case law supports this view; for example, Lord Clarke, in *Gaughran v Chief Constable of the Police Service of Northern Ireland* [2015] UKSC 29, states that: “the rights and expectations of convicted individuals differ significantly from those of unconvicted individuals. The striking of a balance between the public interest and the rights of a convicted or an unconvicted individual will inevitably be appreciably different.”

3.5 The deletion of the custody images of unconvicted individuals should be considered, upon application, on a case-by-case basis. There should be the presumption that the images of those without convictions will be deleted, in line with APP guidance, unless retention is necessary for a policing purpose as set out under paragraphs 2.4 & 2.15.

3.6 This is already the case in a number of other European jurisdictions. It is important to consider and strike an appropriate balance between the protection of personal data and respect for individual privacy with public protection and operational need.

3.7 We have considered whether there would be a benefit in applying a regime similar to the one that operates for fingerprints and DNA, as set out in the Police and Criminal Evidence Act 1984 (PACE) as amended by the Protection of Freedoms Act 2012 (PoFA). However, custody images differ from these biometrics in a number of ways. Firstly, the two types of biometrics are treated very differently under the Act; DNA and fingerprints are generally either destroyed immediately, retained for three years or held indefinitely depending on the seriousness of the offence and whether the individual was arrested, charged or sentenced. However, no specific periods for retention are defined for custody images and no distinction is made based on the seriousness of the offence. Additionally, an image can be considered to be less intrusive than a DNA or fingerprint sample, as faces are generally not private but are, for most people, on display all of the

time (although obviously there are cultural and religious exceptions). This is reinforced by the large number of publicly available facial images on social media, such as Facebook profile pictures. A further consideration is the fact that an individual's DNA profile and fingerprints stay the same indefinitely, whereas generally the usefulness of a custody image decreases over time. Custody images are also used in different ways by the police as compared to fingerprints and DNA, such as for briefing frontline officers and the identification of suspects by witnesses (see paragraphs 6.5 & 6.10).

- 3.8 We also believe that a regime requiring all forces to undertake a weeding exercise of images already held would be unduly complex. From a practical perspective it would be impractical to develop legacy IT systems to identify the stored custody images of those who have or have not been convicted. For example, if forces were required to delete images of those not convicted of the offence in relation to which a custody image was taken, each record would have to be manually examined and deleted. Any routine deletion of historic, or 'legacy', images would therefore be extremely resource intensive, and would, we believe, cost a considerable amount of money to achieve which we believe would be a poor use of taxpayer's money. This would unnecessarily take funding away from other areas of policing, potentially weakening the police's ability to protect the public.
- 3.9 For the reasons outlined under paragraphs 3.7 & 3.8 above this review has concluded that a PoFA style regime for custody images should be rejected.

Deletion of the images of convicted individuals

- 3.10 Generally, over time, the value of custody images decreases. However, it is clear that there are no 'one size fits all' rules as to how long an image will remain useful. **Police forces should continue to have discretion to delete the images of both convicted and unconvicted individuals, as is currently the case under the APP.**
- 3.11 Given that the image of an individual taken when they were under 18 is likely to decrease in usefulness much more rapidly than an image taken when they were an adult, a different approach to retention should apply to these images. There should therefore be a presumption that the images of under 18s will be deleted on review or following an application²⁴.
- 3.12 Convicted individuals should be able to apply for the deletion of their custody image after a period of six (Group 3) or ten (Group 1 or 2) offence clear years have passed since they were convicted. In contrast to unconvicted individuals (with the exception of convicted individuals whose images were taken when they were under 18 and those convicted of a non-recordable offence) there should be no presumption of deletion when a review takes place. In coming to a decision on retention, the factors set out under paragraph 2.10 (for adults) and 2.20 (for under 18s) should be taken into consideration.

Custody images and PND

- 3.13 The variation in the storage and sharing of custody images may already mean that opportunities to identify unknown individuals are being missed.

²⁴ A strong presumption where the under 18 has been convicted of a non-recordable offence

- 3.14 **The use of PND should be further promoted through the National Police Chiefs' Council ('NPCC') lead. The lead should ascertain the future plans of the nine forces who are not uploading custody images to PND.**
- 3.15 **Forces must ensure that they are processing custody images in compliance with the provisions of the Data Protection Act 1998 and other relevant legislation.**

Future systems

- 3.16 **Future local or national IT systems, that will be used for the storage of images, should be designed to integrate relevant data – including court and CPS data – to facilitate a more efficient method of search, retrieval and deletion of images and aim to link and integrate intelligence, crime and prosecution data (subject to relevant legal considerations), and that this should be regularly reviewed.** This will help facilitate a more efficient method of search, retrieval and deletion of images.

Other considerations

- 3.17 The APP guidance should be updated to take account of the review's recommendations on the retention of custody images. Guidance should be clear that police forces must act in accordance with the the DPA, ECHR, and the Equality Act 2010 as well as other relevant legislation. Further, notwithstanding the recommendations made by this review, images may be retained where the individual concerned has given informed consent to this in writing.
- 3.18 **As part of their review of MoPI compliance, chief officers must ensure that they can confidently say whether or not they hold an image of a specific individual and that they consider deletion applications by individuals according to the new retention regime.** Each force is responsible for deleting the images that they upload.
- 3.19 Police systems are changing all the time, and this review has only considered the systems as they stand currently. As HMICS have pointed out in their review, Scotland has different technology systems to those used by forces in England and Wales. This has led HMICS to recommend a different approach to the one put forward by this review. Further, the future National Law Enforcement Data Services (NLEDS) Programme, which may incorporate the National DNA Database (NDNAD), IDENT1, PNC, PND and the Automated Numberplate Recognition Database in a single platform, provides an opportunity to consider more efficient data access, sharing and management of police information. This will help facilitate a more efficient method of search, retrieval and deletion of images.
- 3.20 We appreciate that, for technical and operational reasons, deletion may not always be immediate, but it should take place as soon as reasonably possible.
- 3.21 The DNA Ethics Group was established to provide ethical oversight over the DNA retention regime and was recently expanded to cover fingerprints. The Group has also shown an interest in custody images.
- 3.22 The Digital Ethics Panel for Policing was established by the NPCC in 2015 and seeks to ensure that policing practices are ethically sound.
- 3.23 **The independent Digital Ethics Panel for Policing, in conjunction with the DNA Ethics Group, should consider how they can work together to address the ethical issues relating to the use of custody images.**

3.24 Consideration is being given to extending the Biometrics Commissioner's remit to include oversight of custody images and the Home Office Biometrics Strategy will set out a way forward in this area.

3.25 This review takes account of what is possible at the present time, but as new systems develop, and police practice changes, new considerations may arise. **The custody image retention regime should be reviewed again in 2020.**

3.26 The Home Office has asked the NPCC and the College of Policing to take forward the recommendations in this review.

4. Background

- 4.1 The full scope of the review can be found in the Terms of Reference, set out at Annex A. In completing this review, we conducted research with eight forces in order to understand existing arrangements for capturing, storing, retaining and using custody images. We also conducted literature reviews of forces' retention and use of images, on human recognition ability in relation to images and on emerging technology. Views on existing retention and deletion arrangements of custody images in Northern Ireland, Scotland and other European countries were sought through the police's Criminal Records Office ('ACRO'). A detailed methodology is set out at Annex B.
- 4.2 For the purposes of this review, custody images are photographs of the face of an individual detained at a police station following their arrest, taken by the police under Section 64A of PACE. Custody images are stored by police forces on local custody IT systems and can then be uploaded to PND. Since 2011, most forces' custody images have been uploaded onto PND to increase the ability of the police service to manage and share intelligence and other operational information, prevent and detect crime and make communities safer. Nine forces, including the Metropolitan Police, have yet to upload their custody images. As of July 2016, there were over 19 million custody images on PND, over 16 million of which had been enrolled in the facial recognition gallery making them searchable using facial recognition software.
- 4.3 Since 28th March 2014, it has been possible to search PND for custody images; there are also a small number of local facial searching systems. The previous Biometrics Commissioner, Alastair MacGregor QC, made reference to the new PND search function in his first annual report commenting that "difficult legal, political and other problems may well quickly arise"²⁵.
- 4.4 The retention of such images is governed by the MoPI regime as well as data protection and ECHR considerations. As set out further below, the question of ECHR compliance was considered in detail by the High Court in the case of *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)²⁶ ('RMC').

²⁵ <https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014>

²⁶ <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf>

5. The current legal and operational framework

5.1 Custody images may be taken by the police using their powers under section 64A of PACE. In accordance with PACE, a custody image can be:

- used by, or disclosed to, any individual for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence; and
- after being so used or disclosed, may be retained but may not be used or disclosed except for a purpose so related.

5.2 PACE does not contain any further provisions about the circumstances under which images of arrested individuals can be retained.²⁷ However, MoPI²⁸, issued by the Home Secretary under the Police Act 1996 ('the 1996 Act'), and the accompanying APP guidance set out detailed rules about the collection and retention of personal data (which includes custody images).

5.3 In accordance with section 39A(7) of the 1996 Act, chief officers are required to have regard to MoPI when discharging any function to which the Code relates. MoPI also requires chief officers to "ensure that arrangements within their forces for the management of police information comply with the principles of the Code and with guidance issued under this Code to give effect to those principles."²⁹ Further, chief officers must make sure that their forces adopt practices for the management of information that ensure such information is used effectively for police purposes and in compliance with the law.³⁰ Paragraph 2.2.2 provides that, for the purpose of the Code, 'police purposes' are "(a) protecting life and property, (b) preserving order, (c) preventing the commission of offences, (d) bringing offenders to justice, and (e) any duty or responsibility of the police arising from common or statute law".

5.4 Under the APP guidance, all records that "are accurate, adequate, up-to-date and necessary for policing purposes will be held for a minimum of six years," after which their retention should be reviewed periodically to determine whether their retention is still necessary. This six year minimum "helps to ensure that forces have sufficient information to identify offending patterns over time, and helps guard against individuals' efforts to avoid detection over lengthy periods."³¹ Thereafter, there is a requirement to review whether it is still necessary to keep the record, with scheduled reviews taking place according to the seriousness of the offence. The Home Office and the College of Policing have also produced guidance for forces on the use of facial searches on PND³².

5.5 Any regime governing the retention of custody images must also comply with the ECHR. In particular, Article 8 may only be infringed where this is necessary, proportionate, and in pursuit of a legitimate aim (such as the prevention of disorder or crime). This means that a particular policy or action which interferes with a Convention right must not be arbitrary, unfair, or excessive in pursuit of its intended aim.

²⁷ Albeit paragraphs 5.12 to 5.18 of Code D of the PACE Codes of Practice lay down various requirements concerning the photographing of detainees.

²⁸ <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/>

²⁹ Paragraph 4.1.2.

³⁰ Paragraph 1.1.3.

³¹ APP Guidance, NRAC section.

³² *The Home Office PND Facial Searches Guidance 2014* and the *College of Policing PND Search User Guidance 2015*.

5.6 In 2012, the High Court ruled, in the case of *RMC*, that retention under the Metropolitan Police Service's policy on the retention of custody images of people not convicted of an offence, was a breach of Article 8. In this case, the two claimants, RMC and FJ (who was under 18), had their custody images taken on arrest but no further action was taken against either of them. Whilst accepting that the MoPI regime made some distinction between different categories of offences, the Court considered that it drew no adequate distinction between the convicted and those who are either not charged or are charged but acquitted, and so did not take adequate account of the risk of stigmatisation of those entitled to the presumption of innocence, or the perception that they are not being treated as innocent.³³ Consequently, the court held that the retention of their images "in application of the existing [national police] policy" amounted to an unjustified interference with their right to respect for their private lives and that the policy was therefore unlawful. The Court decided, however, "to allow the defendant a reasonable further period within which to revise the existing policy, rather than to grant relief that might have the effect of requiring the immediate destruction of the claimant's custody images without the possibility of re-assessment under a revised policy".

5.7 Nothing in *RMC* challenges the accepted principle that records of biometric data and custody photographs can make a substantial contribution to law enforcement, the fight against crime, and the exculpation of innocent individuals.³⁴ Further, the courts have also acknowledged, in considering the retention of biometric data by the police, that the impact of retention is less severe in the cases of individuals who have been convicted of an offence than in the cases of those who have not. In both the *Van der Velden* and *W* cases, for example³⁵, the Court held that the interference with the Article 8 rights of convicted individuals was "relatively slight." In addition, it is clear that a scheme of retention which provides for the retention of personal data of those convicted of offences can, in principle, be necessary in a democratic society, in view of the substantial contribution which such records have made to law enforcement in recent years.³⁶

5.8 As well as the specific provisions above, a custody image is deemed personal data under the DPA, and should be processed in accordance with the principles set out in that Act. This means that custody images need to be kept securely, with measures taken to prevent unauthorised access or use, accidental loss or destruction, or any use of the image for purposes incompatible with the purpose for which it was originally taken. As police forces are public authorities, chief officers will also need to consider their duties under the Equality Act 2010.

³³ Paragraph 54 of *RMC*.

³⁴ See, for example, *R (S) v Chief Constable of South Yorkshire Police* [2004] UKHL 39, [2004] 1 WLR 2196, paragraph 2 *per* Lord Steyn (attached at Annex 5); *Gaughran v Chief Constable of the Police Service of Northern Ireland* [2015] UKSC 29, [2015] 2 WLR 1303, paragraphs 40 and 41 *per* Lord Clarke JSC.

³⁵ Application No 29514/05, *Van der Velden v The Netherlands* (7th December 2006), Application No 20689/08, *W v The Netherlands* (20th January 2009).

³⁶ *Van der Velden* and *W*.

6. The use and administration of custody images

Capture and quality assurance of custody images

- 6.1 There are a number of differences in the ways that forces capture and upload custody images. Three of the eight forces who participated in the field research take images using a camera or webcam connected to a computer with detainees sitting with their backs against the wall in the custody suite, and three use a photo booth. Five forces retain one image per arrest (all front facing), whilst one force stores three (a front facing, left facing and right facing profile). Work is underway to examine the value of extending this to five images, as is done in Germany, or even to collect a single three-dimensional image. Forces use varying record management systems for capturing and retaining custody images. Variation in practice in capturing and storing custody images can impact upon the quality of images.
- 6.2 All forces surveyed stated that they comply with national standards in relation to the quality of custody images. These standards were originally developed by the Police Information Technology Organisation ('PITO') and endorsed by the National Police Improvement Agency ('NPIA') and ACRO in 2008. Forces are generally compliant with national standards although there is some room for improvement. **Chief officers must ensure that national standards on custody image collection are adhered to.**
- 6.3 There is some variation in the routine monitoring of image quality. One force centrally audits the quality of images taken on a daily basis, and in another, the quality of images is monitored by those who capture them, and is part of Key Performance Indicators for staff, with retraining provided to those who fall below the standard.

Police use and management of custody images

- 6.4 The total number of images stored by each force involved in the field research ranged from 26,816, in the smallest of the eight forces, to 7.8 million³⁷ in the largest. Forces may have additional copies of the same image on multiple systems or additional images on legacy systems. Most of the 43 territorial police forces (plus the British Transport Police) store custody images on Niche, Athena or the National Strategy for Police Information Systems ('NSPIS') systems. The Athena system can allow images to be retained and deleted to pre-set criteria, (such as time retained); however, this capability needs to be enabled by individual forces.
- 6.5 Custody images are a standard feature of everyday policing. They are commonly used in briefing frontline officers so they can identify suspects, offenders or arrestees on bail. Custody images also feature in investigations through witness identification in photo-books and searching for unidentified suspects against databases of custody images. To support and equip frontline officers, daily shift briefings use custody images to inform officers who to look out for such as wanted offenders, individuals who have failed to answer bail or those who pose a risk to the public. Custody images may be the only image of a suspect held by the police so they are key to allowing witnesses to make identifications, particularly in historic cases.
- 6.6 Custody images are also used to develop leads within investigations. They can be searched against other images of suspects, such as those obtained from CCTV, either manually or through facial searching on PND. The identification of an individual through a custody image is often followed by an identification parade with a witness or victim.

³⁷ As at March 2015.

- 6.7 Custody images are also used administratively, for example in identifying detainees who it is believed have given a false name, recording the physical condition of detainees when brought into custody, media briefings and in the identification of dead bodies.
- 6.8 Other, less common, uses include providing assistance to other agencies (such as those connected with immigration) in identifying individuals, assisting investigations in other countries through the International Criminal Conviction Exchange and for use as evidence in court proceedings. Custody images, however, are not considered to be definitive evidence of identification as might be the case with other biometrics such as fingerprints and DNA.
- 6.9 Where the police hold multiple images taken on different occasions, they may show changes in appearance over time. This can help, for example, in ageing photos of missing individuals and in identifying drug use.
- 6.10 Field research, confirms that custody images have a range of uses and that they play an important role in protecting the public. In many instances, highlighted by forces, the image was the sole means of identifying an offender, often for a totally unrelated crime, and often long after the offence for which the original image was taken.

Custody images and PND

- 6.11 PND went 'live' in 2010. It was developed following recommendations³⁸ made by the 2004 Bichard Inquiry into the Soham murders of 2002, and its findings that forces in England and Wales were unable to search other forces' intelligence on a particular individual easily, or to be informed actively if a force had intelligence about any specific individual.
- 6.12 PND offers a national capability for the police to share, access and search information which was previously only held locally by individual forces, thereby overcoming geographical and jurisdictional boundaries. It allows the police to share "information and intelligence on a national basis...to safeguard children and vulnerable people, to counter terrorism, and to prevent and disrupt serious and organised crime³⁹." It should be noted that PND is not an evidential system, but a system designed to facilitate the sharing of intelligence.
- 6.13 The PND facial searching facility allows an authorised user (usually a police officer), who has already tried to identify an individual through the Police National Computer ('PNC') and other relevant systems, to search through saved custody images ('gallery images'), to find potential matches against an image that they have temporarily uploaded (a 'probe image').⁴⁰ Facial searching is limited to images of a specified size range (10KB to 5000KB). The search will return a maximum of 50 potential matches (although zero matches are not uncommon) ranked in order of closeness of match. Officers must then consider the potential matches, assessing the likelihood that the image is a match, possibly using associated intelligence from PND. As such, facial searching is not automated facial recognition, but a tool to make manual searching more efficient. The results – rather than an individual identification – amount to intelligence.

³⁸ "Recommendation *1: A national IT system for England and Wales to support police intelligence should be introduced as a matter of urgency".

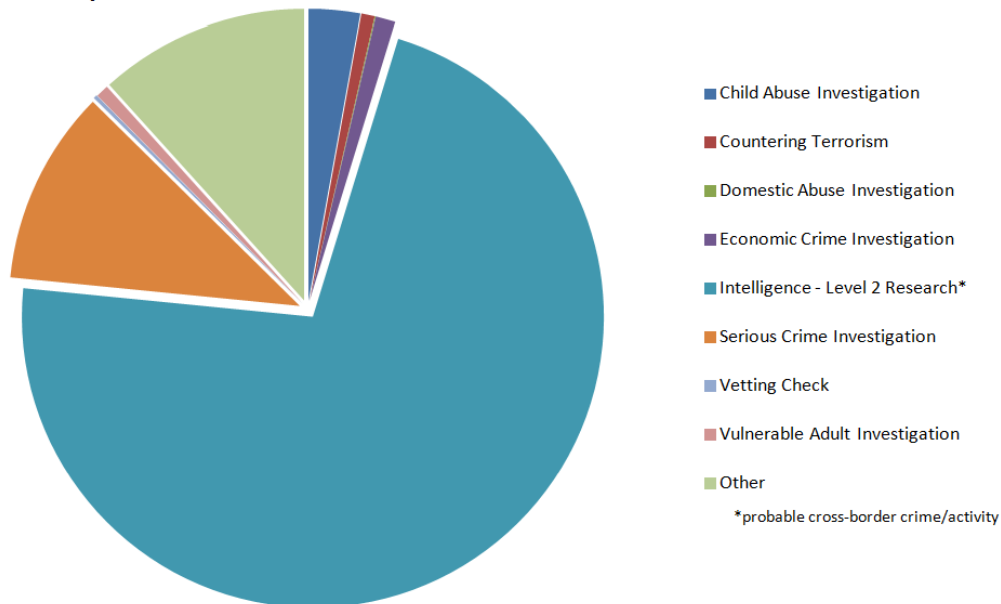
³⁹ http://www.college.police.uk/What-we-do/Learning/Curriculum/ICT/PND_Police_National_Database/Pages

⁴⁰ The probe image is not retained on PND.

6.14 Forces who took part in the research indicated that if they needed to search an image, for use in an investigation or interview, they would generally start by looking on their local systems and only revert to PND if the local system did not contain an image they could use.

6.15 All but nine forces upload custody images to PND, and some fifty agencies run searches through PND, including police forces in Northern Ireland, Scotland, England and Wales and organisations such as the Ministry of Defence and the National Crime Agency. Of the nine forces not uploading images, the largest is the Metropolitan Police. As of July 2016, there were over 19 million custody images on PND. This will include duplicate images from individuals due to multiple arrests by the same force, and potentially by different forces; hence the number of images does not relate to the number of individuals whose image is held on PND. Images can be searched by any of over 8,000 holders of a PND licence⁴¹ issued with every search being recorded against the individual user making them fully auditable. According to recent data, the top reasons for facial searching on PND were for potential cross-border crime (72%) and for serious crime investigation (11%).

Searches shown by PND Search Reason Code 1 Jun-18 Nov 2015



6.16 It is important that decisions on the ways in which images are collected, stored and compared – and the length of time for which they are retained – do not preclude the take-up of technological advances which may play a significant role in the prevention and investigation of crime and the presentation of evidence in courts. With improving image quality and search algorithms, facial searching is used more and more in policing. As the case studies below demonstrate, adding this capability to PND has already significantly improved the police’s ability to protect the public, in ways that would not previously have been possible.

⁴¹ Access to PND is restricted to authorised individuals only. Users are required to apply for a PND license and are vetted and trained before they can use PND.

Case Studies – Facial Searches

A man arrested for immigration offences was not charged or convicted and so his fingerprints and DNA were destroyed. He was later arrested for cannabis farming and gave a false name. His biometrics showed a 'no trace', but when his image was searched against PND, officers were able to ascertain his real identity. He was convicted and received a six month term of imprisonment.

A raid on the premises of an organised crime group found a number of forged identity documents with false names. Using the images, and searching against PND, police identified 24 of the individuals.

DNA evidence identified a possible rapist in an 18 year old 'cold case' but the victim had since died. Further investigation uncovered another case with a similar modus operandi. Using a custody image of the suspect from 18 years previously for an unrelated vehicle crime, the police were able to get a positive identification in a still image parade. The suspect was convicted and given an 18 year term of imprisonment.

An image on the mobile phone of a witness to a murder, when searched in PND, enabled police to identify the last individual to see the victim, who was later arrested and charged with their murder.

An investigation uncovered an image showing sexual exploitation of a child. It also showed the offender's face; by using a search on PND police were able to identify the offender from the image.

A man sexually groomed a child over Skype. The account details and email failed to give identification but a PND facial search on the Skype profile picture identified the offender.

A murder suspect, identified only by a social media nickname in an anonymous call, was positively identified after running a facial search on their social media profile picture.

A theft occurred in a bookmaker in Durham, where CCTV showed the suspect leaning over the counter and removing money from the till. Durham police conducted a PND Facial Search, which led to further enquiries that suggest the suspect had been arrested by Devon and Cornwall police the week before and was known to Surrey police. The image on PND had been uploaded by Police Scotland the year before. The suspect was arrested, admitted the offence and was charged. He pleaded guilty in court and was sentenced to 6 weeks imprisonment and ordered to pay compensation to the bookmakers.

6.17 There are also a small number of search systems used by individual forces, which are regulated by the same legal framework, under the MoPI regime and the DPA. For example, Leicestershire Police use a commercially available tool used in many countries around the world. Because the system works only in the local force area (not PND), they have greater control over the quality of the images that are searched against, and so a higher success rate for searches, although no ability to search for photos stored by other forces.

Other jurisdictions' retention of custody images

6.18 In Scotland, the Criminal History System ('CHS') records the outcomes of cases and retains information based on the nature/seriousness of the crime. Custody images are not uploaded to CHS unless an individual is charged with a crime and will be deleted from both CHS (and PND) within six months of an investigation concluding if there is no conviction. Custody images of an individual convicted are retained on CHS, and therefore on PND, in accordance with the rules on retention for fingerprints and DNA set out in the relevant Scottish legislation. Custody images are also retained on local systems for either six years (for 'volume' crime) or twelve years (for serious crime) in accordance with data retention policies but these are not uploaded onto PND. If the reviewing officer decides that certain records need to be kept for a longer period, a justification is provided and a time limit set on a case by case basis. Her Majesty's Inspectorate of Constabulary in Scotland (HMICS)⁴² has recently completed a review of Police Scotland's usage of PND, including how images are used and stored. The report recommends that the Scottish Government legislate to place these arrangements on a statutory footing in Scotland. The Scottish Government is presently considering whether to take these recommendations forward.

6.19 Every European Union (EU) Member State has its own laws and policies with regard to the taking and retention of images following arrest. Those countries with national identification photo cards, where law enforcement agencies have access to the database on which they are stored, may well not be concerned with the retention of arrest images once identity has been established. Many EU Member States maintain a position whereby, upon a No Further Action or Acquittal decision, the image is deleted upon the request of the subject. However, the minimum period before this request can be made varies from immediately following the decision (Belgium, Cyprus, Czech Republic, Hungary, Ireland, Italy, Netherlands, Slovenia, Spain and Sweden) to one year (Malta and Finland). France is currently undertaking a review of its retention law but at present, custody images are stored for 25 years unless the subject requests the deletion, in which case the prosecutor decides whether or not to require it.⁴³

⁴²<http://www.hmics.org/publications/hmics-audit-and-assurance-review-use-facial-search-functionality-within-uk-police>

⁴³ *Review of European Union Member States Position with Regard to the Retention of Custody Photographs and Other Biometric Data* (ACRO, 2015) (unpublished)

Annex A: Review of legal base, regulation, governance and procedures for the use and retention of custody images

Terms of reference

1. Issue

- 1.1 The legal basis for, and appropriate regulation of, the use and retention of custody images taken by the police and their further processing on national and local systems; and governance, oversight, policies and guidance at a local and national level.
- 1.2 Custody images are taken under S64A of the Police and Criminal Evidence Act 1984 (PACE). The scope of this review expressly excludes images which were primarily gathered as intelligence and/or are held as evidence. This is because such images are held as police information or evidence in relation to specific events, rather than for verification.
- 1.3 Defined in the Code of Practice on the Management of Police Information 2005 (MOPI) paragraph 2.2.2 as (a) protecting life and property (b) preserving order (c) preventing the commissioning of offences (d) bringing offenders to justice, and (e) any duty or responsibility of the police arising from common or statute law.
- 1.4 The Code of Practice on the Management of Police Information (MOPI) was issued in 2005, and this is now supported by detailed guidance issued as Authorised Professional Practice (APP) by the College of Policing.

2. Objective

Provide advice to Ministers on:

- 2.1 The current legal and operational framework, including relevant guidance on procedures, and whether they adequately address relevant case law developments in relation to the right to respect for private and family life as set out in Article 8 of the European Convention on Human Rights;
- 2.2 The utility and benefits of custody images in meeting policing purposes 2 and expected future developments in their use, including automated facial recognition systems, and;
- 2.3 Options for change where this appears necessary in relation to legislation, regulation, governance, oversight, policies and guidance.

3. Scope

The review will engage with key partners and take account of:

- 3.1 Examination of the **legal framework** for custody image retention and use, including the Data Protection Act 1998, the statutory code of practice made under S39A of the Police Act 1996 and associated guidance 3 and relevant case law relating to interference with Article 8 rights;

- 3.2 The various **purposes and use cases** for which the police make use of custody images and associated benefits and risks. For example, identifying unknown persons from CCTV images, preparation of video identity parades, or the preparation of alerts relating to known suspects;
- 3.3 An assessment of whether custody images should be treated in the same way as other **biometric identifiers** such as DNA profiles or fingerprints, or if (whether as a result of differences in their operational usage and utility or otherwise) they should be subjected to different retention regimes. This might take account of (i) quality standards for data capture (ii) potential for use by humans (iii) the validity of algorithms for automated searching and matching (iv) the stability of biometric data representations over time and (v) the proposition that searchable databases of custody images represent a greater threat to individual privacy than searchable databases of DNA profiles and fingerprints;
- 3.4 Examination of **retention regimes** and their proportionality (including in particular the relationship between any given retention regime and the risk presented by relevant individuals), of **governance arrangements** as regards the retention and processing of custody images at a local and national level, of any appropriate comparators (including any international comparisons), and of any implications for the roles of the Information Commissioner, the Biometrics Commissioner or other regulatory bodies;
- 3.5 **Societal views** on the use and retention of custody images;
- 3.6 Examination of **current local force arrangements** for storage, processing, distribution and linking of custody images to other police records, including use of automated facial recognition systems;
- 3.7 Examination of **current national arrangements** relating to the uploading of custody images to the Police National Database (PND), and the search and matching of images of unknown persons against the uploaded custody images, and any existing links to other national systems;
- 3.8 **Horizon scan** of technological developments and opportunities and of plans for further sharing and utilisation of custody image data across local or national systems.
- 3.9 Potential **implementation costs, benefits and affordability** associated with emerging options to strengthen or amend the relevant statutory base, governance arrangements, guidance or procedures to ensure that policing benefits associated with the retention and use of custody images can be realised with public support and confidence and without disproportionate interference with Article 8.

4. Product

- 4.1 The review will report to Ministers in spring 2015 with an assessment of options for the way forward. The report should also set out any routes to implementation and the risks attached to each option, along with requirements for any necessary or appropriate consultation and any need for primary or secondary legislation, or amendments to statutory codes or guidance. The report may also make recommendations about the need for further work to review any emerging implications for, or potential impact on, the legal base, governance, policies and/or procedures relating to other categories of police information

Home Office
11 March 2015

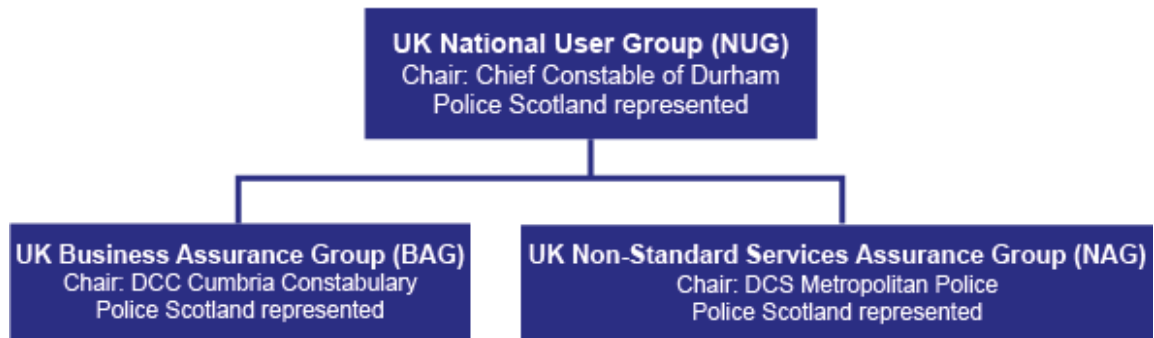
Annex B: Methodology for the custody image review

1. Crime and Policing Analysis (CPA) Unit were commissioned to conduct a field search with sample forces to identify the various purposes and use cases of the custody images and the related benefits and risks. The sample included:
 - Metropolitan Police (largest force. Also has own facial recognition software);
 - Essex (Force with Athena system, a single IT system managing police investigations, intelligence and defendants (both custody and case preparation));
 - North Wales (rural force);
 - Thames Valley Police (TVP) (Force with Niche, a records management system);
 - Leicestershire (own facial recognition facility);
 - City of London (CoL) (fraud focus and do not upload to PND);
 - Merseyside (urban force with own facial recognition software); and
 - Durham (Chief Officer is the National Policing Lead for this area).Written submissions were sent in by some forces and telephone interviews were also conducted to follow up on received responses as well as to obtain answers to questionnaire. The results from this were validated at a practitioner level workshop to confirm understanding.
2. CAST and CPA submitted a literature review on:
 - evidence base for human recognition ability;
 - validity of AFR algorithms and what variables have an impact on successful matching;
 - comparison between controlled environment of e-passport gates and CCTV gathering in uncontrolled conditions;
 - data point stability (and why ten year renewal of photos for passport and DVLA); and
 - horizon scanning.
3. Views were sought from England and Wales through the fieldwork on the retention regimes and Governance. ACRO supported in getting the views from NI, Scotland and other European jurisdictions.
4. Communication Directorate were commissioned to run media scans on cyber space to find out what if anything has been said about custody images.
5. We have collaborated with PND Live Services to understand the arrangements with up-loading to PND and the uses of this.
6. We have consulted with legal advisers.

Police Science & Technology Unit
2 September 2015

Annex C: Governance of PND

UK Governance arrangements for PND



Annex D: Review of published information relating to the civil liberties/privacy implications of the retention and use of custody images

Privacy and civil liberties

Roberts (2001) outlined the difficulties of privacy in English law. He suggested, however, that legal recourse to the 'right to privacy' in England and Wales had been clarified following the incorporation of the ECHR, through the Human Rights Act 1998.

Williams et al (2004), writing on the arguments around the construction of a national DNA database, noted that Article 8.1 of the ECHR stated that: 'Everyone has the right to respect for his private and family life, his home and his correspondence'. However, this was a 'qualified right' which needed to be balanced against the rights of others or wider societal interests. In other words, any judgements made in light of the ECHR had to take into account, not only the right to privacy of individuals, but also collective interests (which in the context of the retention of custody images might be seen as the police's ability to protect the public).

Williams and Wienroth (2014) acknowledged the success of the use of DNA, although they highlighted the significance of due process and human rights challenges to the increasingly routine use of DNA databases. As such, the civil liberty and privacy arguments given below were not considered in isolation from the operational policing benefits as outlined in the first section of this review.

Michael and Bronitt (2012), writing on the relationship between technological development and the law, specifically in the context of increased use of CCTV, said that 'law disciplines technology', in that it provides a framework in which technology can be used. They argued, however, that the law was only able to do this in a partial way given that technology outstripped the capacity of law to regulate it (i.e. technological developments happen fast, with the law having to keep up with them).

They further argued that the rise of new technologies posed a substantial threat to human rights as technology might be used before relevant human rights considerations had been fully debated. They cited the increased use of CCTV, and audio-visual recording and tracking devices, which they suggested significantly widened the scope of the state and businesses to intrude into the lives of citizens. As set out below, similar arguments have been made in relation to the retention of custody images.

The Biometrics Commissioner, in his 2014 Annual Report⁴⁴, stated that he was "acutely conscious" of the contribution custody images, and the project seeking to enhance facial search technology, could make to the prevention and detection of crime, whilst outlining the necessity of adhering to wider consultation and specific legal advice. He believed a new regulatory regime was necessary in order to establish the balance between "the public interest in the prevention and detection of crime; and the individual's right to privacy, particularly in circumstances where that individual has never been convicted of an offence".

A 2013 House of Commons Science and Technology Committee report⁴⁵ underlined how useful custody images could be in assisting the police in investigations, whilst expressing concern that an appropriate regulatory regime had not yet been put in place following the

⁴⁴ <https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014>

⁴⁵ <http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/73402.htm>

High Court ruling in *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 168.

The *RMC* case referred to was brought against the Metropolitan Police by two individuals who contested the retention of their custody images. The claimants had each been arrested on suspicion of an offence, but were not subsequently proceeded against. They made the claim that once the decision was taken not to proceed against them, retaining their custody images was a breach of their rights under Article 8 of the ECHR. The High Court ruled in the claimants favour, deciding that the retention of their custody images did indeed breach these rights.

The judgment stressed what the court considered to be the similarity between fingerprints and images in that they contained “external identification features”. The Metropolitan Police had argued that images were quite distinct from fingerprints, in that fingerprints have an “objective and irrefutable” character, but the court rejected that contention. The court concluded that the retention of the custody images constituted an interference with the right to respect of private life.

The question is not over the use of the images themselves, but rather what the appropriate legal framework for their use should be. Indeed, even within organisations that focus on human rights, there is a recognition that using images is necessary, but that there must be appropriate governance and legal recourse for individuals if they feel their images have been kept or used inappropriately. For example, Emma Carr, Acting Director of Big Brother Watch (a human rights campaign organisation), suggested that facial recognition technology should be used only with a “high level of accountability and oversight”, and added that it was essential that “people are able to access meaningful redress when they feel their privacy is infringed (BBC, 2014)”.

The Biometrics Commissioner, in his 2014 report, stated that “proper consideration should now be given to the civil liberties and other issues that arise as regards those newer technologies and urgent steps should now be taken to ensure that they are governed by an appropriate regulatory regime” and “although a searchable police database of facial images arguably represents a much greater threat to individual privacy than searchable databases of DNA profiles or fingerprints, this new database is subject to none of the governance controls or other protections which apply as regards the DNA and fingerprint databases by virtue of PoFA”

The report from the House of Commons Science and Technology Committee also expressed concerns about the civil liberty implications of the police use of custody images in the absence of an appropriate legal framework. The report emphasises, in particular, what it saw as the problematic nature of the uploading of images to, and use of facial recognition technology in, PND, especially given that this included images of people not subsequently charged with, or convicted of, a crime. It cited the fact that the High Court ruling in 2012 found that existing policy concerning the retention of custody photograph by the police was “unlawful”, but that appropriate legislative development had not subsequently taken place.

The Joint Committee on Human Rights (cited in Williams et al, 2004) highlighted the risk that the arrangements for managing the large volume of personal data available through a national DNA database posed and raised issues with regard to compliance with ECHR Article 8 (the key consideration in relation to the High Court ruling on the retention of custody images).

Williams and Wienroth (2014) accepted the importance of DNA to police investigation, but highlighted the human rights implications of its increased use. They found that there was

broad agreement that custody images were of significant operational importance to the police, but that, similar to DNA retention, this should be weighed against civil liberty issues.

Blakemore and Blake (2012) noted that, in 2008, the European Court of Human Rights ruled that 'blanket retention' of DNA and fingerprints by the UK on the NDNAD was contrary to Article 8. This led to a legislative review and consultation and, ultimately, two Acts of Parliament: the Crime and Security Act 2010 (although the provisions of this act were never brought into force) and PoFA, which restricted the retention regime for DNA and fingerprints.

Williams et al (2004) identified that the main objection to NDNAD was not the taking of samples but the retention, and searching of DNA profiles of those who had not been convicted of or charged with an offence. They quoted the then MP, Simon Hughes, as saying that the Government had accepted that those who had never been detained by the police had the right to resist having their DNA taken and stored without their authority, and that this placed them in a different category from those who had been detained, but not proceeded against, or found not guilty in court. Their contention was that the second group should be presumed to be as innocent as someone who had not been investigated and that the differentiation that they saw as existing prejudiced this group and gave them a status with the authorities that disadvantaged them in terms of their freedom and liberty.

They also quoted the campaign group Liberty as referring to those who had been detained, but not convicted as 'innocent ex-suspects', but contended that this differentiation, between convicted and non-convicted persons, was "blurred by the inclusion on the database of one-time suspects", and that this was the central challenge of the arguments around DNA retention. However, they cited a 2004 Court of Appeal ruling setting out a different concept of 'innocence'; that in the eye of the law, everybody is innocent unless they have been convicted of an offence, but from a policing and law enforcement perspective those unconvicted do not necessarily remain beyond suspicion. Indeed, the ruling suggested they cannot be if policing is to operate effectively given that for detection "ordinarily begins not with proof but with inquiry".

Human ability to recognise individuals from images

Hancock et al (2000) suggested that people are 'excellent' at identifying faces familiar to them, even from very low quality images, but are bad at recognising, or even matching, unfamiliar faces. This first point suggests that even if an image is of a low quality then there is a good chance of a positive match if the individual doing the identification is familiar with the subject. However, it is clearly the case that in the police use of images, whether they be for witness identification or police officer briefings, that the subject will not always be familiar to the individual viewing the image so differences in recognition of unfamiliar persons are relevant.

Davis and Valentine (2015) sought to test the theory that when high-quality images of an offender are available, identity verification should be relatively straightforward, irrespective of familiarity. However, they highlighted research showing that the "identification of unfamiliar people is often unreliable, even when there are no memory demands and the high-quality images to match are taken at approximately the same time with no attempt to change appearance". This means that the matching of unfamiliar faces can be unreliable even when people are asked to match images in real-time, as opposed to having to remember those shown to them previously, and there is little difference in the appearance of the subject between images (more will be said below about differences between images of the same individual).

Bruce et al (2001) conducted an experiment where participants were shown a series of pairs of facial images, firstly from poor-quality CCTV, and secondly a high-quality custody image. Participants had to report on whether they showed the same individual or not. With images of the same individual, correct identification varied dependent on whether they were familiar with the people in the images or not (93% and 76% respectively). Where images were of different people, this was correctly identified 91% of the time with familiar and 55% of the time with non-familiar images.

55% is not much higher than might be expected by chance, so this does suggest that people's ability to correctly identify that two images are not of the same individual if they are unfamiliar to them is limited. Clearly the different individuals in the images cited here were fairly similar in appearance, but it might be argued that this is exactly the kind of differentiation that might often be necessary within police work (i.e. if images are very obviously of different people, identification is not necessary).

There is also evidence to suggest that if those viewing images were not previously familiar with the individual in the image, bias may be introduced if substantial time is spent "viewing and analysing photographic images from the scene" (Davis and Valentine, 2015). Indeed, even identification 'experts' may display "cognitive biases" leading to incorrect identifications, and so previous information about a case might influence judgements (Cole and Thompson, 2013). It is possible when images are repeatedly viewed individuals "will be vulnerable to such biases by ignoring 'exculpatory' visual cues in some frames that do not match the appearance of the defendant, while giving greater weight to alternative frames as there appears to be a greater similarity of appearance between the defendant and the individual depicted" (Davis and Valentine, 2015, p. 217)".

Differences between the particular view of an individual or their facial expressions might also make a difference to the accuracy of the identification. Police custody images are normally all front facing and this may be relevant when comparing them to a probe image (such as one taken from CCTV).

Estudillo and Bindemann (2014) explained how variation in the orientation of an image could make a significant difference to the appearance of an individual's face. For example, although a front facing image might show a pair of eyes and a 'symmetrical mouth and nose', these features might not be fully visible in a side facing image. This variation, whilst less problematic when viewing images of people who are familiar could cause problems with the identification of unfamiliar people.

Bruce (1982) demonstrated that identifiers recognise 90% of faces when they are shown images from the same view. However, "accuracy declined dramatically, to just 60%, when recognition memory was subsequently tested across a change in view" (Estudillo and Bindemann, 2014, p. 589). This implies that when custody images (all of which are front facing), are more likely to lead to an accurate identification of an individual than if images where the face is at an angle are used, even if the subject is unfamiliar to the identifier. Changes in facial expression from neutral to smiling also significantly increased the likelihood of error.

The findings also showed that when an eye witness is asked to make an identification from a custody image of someone they have seen in real life, accurate identification is more likely than when custody images are compared to an image from another source, for example CCTV.

There is also evidence to suggest that individuals may find accurate identification more problematic if an image is of someone from a different ethnicity. Davis and Valentine (2015) demonstrated that such differences had been extensively replicated in experiments and that

“people tend to be better at recognising individuals from their own ethnicity than those from other ethnicities”.

Nakabayashi et al (2010) reported similar findings, which they referred to as the ‘other-race effect’. They suggested that this might lead to either a wrongful conviction or to a failure to prevent the suspect from carrying out a crime. Of course, this will only be the case in a limited number of identifications conducted through the use of custody images but it does appear to be a significant factor in such cases.

Some research suggests that an individual’s identification of an individual from an image may be less accurate depending on what contextual information is supplied to them. Writing on the case of Jean Charles de Menezes, who was incorrectly identified by police officers based on a range of images they had seen of a different individual, Davis and Valentine (2015) explained that officers were told that the suspected individual might have purposefully changed his appearance and that the images they viewed demonstrated this. Such factors have been shown to create a ‘liberal response bias’ whereby “being told that two dissimilar images depict the same individual may have been interpreted as an implicit instruction that de Menezes’ appearance had changed, and to therefore be more ‘flexible’ when making their identification judgements”.

Horry et al (2014) conducted research on video identification procedures, though they stress that their findings also apply to identifications made via images. They pointed out that the PACE Codes of Practice stated that “if they [the witness] cannot make a positive identification, they should say so” (PACE Code D, Annex A, paragraph 11).

However, they stated that there could be variation in the understanding of what a positive identification meant in practice and that this could impact on whether or not one was made. They cited research conducted by Hughes (2005) in which 30 police identification officers were interviewed where a large variation was observed in terms of responses to what was understood by positive identification, with every officer having a different understanding of the term. They suggested that if this difference of opinion existed amongst police officers then it must also exist amongst witnesses who were asked to make positive identifications.

This suggests definitions of positive identifications can impact on a cognitive decision and that therefore recognition is linked to definitions and understandings. They also noted a similar effect in terms of cognitive decision making in terms of the way the police administer identifications made through images. They noted that the PACE Codes stated that “care must be taken not to direct the witness”, and officers should not give “attention to any one individual image or give any identification of the suspect’s identity” (PACE Code D, Annex A, paragraph 13). However, they contended that in some cases, officers might subconsciously influence witnesses, for example that a “slight pause, a raised eyebrow, a brief smile – all of these things could be interpreted by an eyewitness as an indication of the suspect’s identity”. They also noted the potential impact on recognition in events that are observed by multiple eyewitnesses. In such cases, eyewitnesses might discuss the event with one another and this could lead to convergence in their ‘memory reports’ of the incident. They termed this ‘memory conformity’ and it occurs because memory is ‘reconstructive’ i.e. when someone is asked to remember an individual through the viewing of an image, that memory is reconstructed, and can be changed in some way to incorporate information from other sources.

References

BBC (2014). Leicestershire Police trial facial recognition software –

<http://www.bbc.co.uk/news/uk-england-leicestershire-28307938>

Blakemore, B. and Blake, C. (2012). Can the National DNA Database be Effective and Comply with Human Rights Legislation? *The Police Journal*, 2012 - vathek.org.

Bruce, V. (1982). Changing faces: Visual and non-visual coding processes in face recognition. *British Journal of Psychology*, 73, 105–116.

Bruce, V., Henderson, Z., Newman, C., & Burton, A.M. (2001). Matching identities of familiar and unfamiliar faces caught on CCTV images. *Journal of Experimental Psychology: Applied*, 7, 207–218.

Cole, S.A., & Thompson, W.C. (2013). Forensic science and wrongful convictions. In C.R. Huff, & M. Killias (Eds.), *Wrongful Convictions & Miscarriages of Justice* (pp. 111–135). London: Routledge.

Davis, J.P., & Valentine, T. (2015). Human verification of identity from photographic images. In T. Valentine and J.P. Davis (Eds.), *Forensic Facial Identification: Theory and Practice of Identification from Eyewitnesses, Composites and CCTV*. Chichester: Wiley-Blackwell.

Estudillo, A. J., & Bindemann, M. (2014). Generalization across view in face memory and face matching. *i-Perception*. (2014) volume 5, pages 589–601

Hancock, P. Bruce, V. and Burton, A. (2001). *Trends in cognitive sciences* 4 (9), 330-337, 2000.

High Court of Justice (2012). *R (on the application of) RMC and FJ -v- Commissioner of Police of the Metropolis and Secretary of State for the Home Department and Liberty and Equality and Human Rights Commission*.

Horry, R. Memon, A., Milne, R., Wright, D., and Dalton, G. (2014). Video Identification of Suspects: A Discussion of Current Practice and Policy in the United Kingdom. / In: *Policing: A Journal of Policy and Practice*, Vol. 8, No. 1, 2014, p. 35-42. Saved in folder -

http://pure.rhul.ac.uk/portal/files/23302843/Policing_2013_Horry_police_pat008.pdf

House of Commons Science and Technology Committee (2014). *Current and future uses of biometric data and technologies*, Sixth Report of Session 2014–15.

Joint Committee on Human Rights (2003). *Criminal Justice Bill: Further Report*. London, House of Commons, House of Lords, The Stationery Office Limited.

MacGregor, A. (2014). *Commissioner for the Retention and Use of Biometric Material: Annual Report 2014*. Her Majesty's Stationery Office.

Memon, A., Havard, C., Clifford, B., Gabbert, F., and Watt, M. (2011). A field evaluation of the VIPER system: A new technique for eliciting eyewitness identification evidence. In: *Psychology, Crime and Law*, Vol. 17, No. 8, 2011, p. 711-729.

Michael, K. and Bronitt, S. (2012). "Human Rights, Regulation, and National Security" IEEE Technology and Society Magazine 31.1 (2012): 15-16.

Available at: <http://works.bepress.com/kmichael/264>

Nakabayashi, K. Memon, A. and Lloyd-Jones, T. (2010). Recalling and recognizing faces of own- and other-race: a behavioural and eye movement study:

<http://www2.hull.ac.uk/science/psychology/research/cognition/recallingandrecognisingfaces.aspx>

Roberts, P. (2001). "Privacy, Autonomy and Criminal Justice Rights: Philosophical Preliminaries" in Peter Alldridge and Chrisje Brants (eds), *Personal Autonomy, The Private Sphere and the Criminal Law: A Comparative Study* (Hart Publishing, 2001), 49-78.

Williams, R. Johnson, P. and Martin, P. (2004). 'Genetic information and crime investigation: social, ethical and public policy aspects of the establishment, expansion and police use of the National DNA Database.', Project Report. Durham University, School of Applied Social Sciences, Durham.

Williams, R. and Wienroth, W. (2014). DNA Technology and Police Investigations - *Encyclopaedia of Criminology and Criminal Justice*, 2014, pp 1128-1136

International Standard Book Number: 978-1-78655-382-9