Independent Advisory Group on the Use of Biometric Data in Scotland

March 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

Table of Contents

Introduction

In May 2017, I was asked by the Cabinet Secretary for Justice to chair an Independent Advisory Group to review the retention of custody images by Police Scotland. The Cabinet Secretary for Justice also asked that the Group consider the use and retention of biometric data more generally in policing to seek to establish an ethical and human rights based framework which could be applied to existing, emerging and future biometrics in what is an important and fast-moving area of technology.

The present review comes at an opportune moment as it allows the position in Scotland to continue to be developed in a principled manner which gives appropriate weight to considerations of public protection and security on the one hand, and privacy and other relevant human rights and ethical considerations on the other. Such development should proceed on the basis of as much public awareness and engagement as possible, to try to ensure that there is appropriate public confidence and trust in technology and data which will be used increasingly, and which is important to society as a whole.

From the perspective of knowledge, experience and continuity, we have been fortunate in our work to have as Advisory Group members Her Majesty's Chief Inspector of Constabulary in Scotland, Derek Penman, and Professor Jim Fraser. Their reports in this area, described in more detail below, have been key in developing the current landscape and outlining a principled course for the future. In addition, we had the assistance of Dr Brian Plastow who worked on the report by Her Majesty's Inspectorate of Constabulary in Scotland (HMICS). Brian's knowledge and enthusiasm have been invaluable.

We also had the benefit in membership of our Group of considerable knowledge, experience and expertise in the fields of policing, forensic science, criminal justice, data protection, human rights and quantitative research. I am grateful to all Advisory Group members for their contributions. This report could not have been produced in such a short period of time without considerable effort on their part.

The Group had six months to carry out its work. The final report was submitted to the Cabinet Secretary for Justice on 7 February 2018.

The Scottish Government has advised that it intends to undertake a public consultation later in 2018 which will include discussion of our recommendations. We did, however, seek views from a broad range of interested and expert parties, both individuals and groups. We identified them with the assistance of those working in the field of biometric data and through responses to previous relevant consultations. A list of those who responded and consented to being identified is attached at Appendix 3. We are extremely grateful to those who took the time to send us written submissions. Their submissions have greatly assisted us in producing our recommendations. Written responses and submissions will be published along with this report.

In addition, many individuals gave up their time to speak to us in meetings and telephone calls, as well as sending us papers and suggestions. Special mention should be made of Professor Paul Wiles, the UK Biometrics Commissioner[1], and Dr Gill Tully, the Forensic Science Regulator (England and Wales)[2]. Both attended one of our Group meetings, along with Dr Carole McCartney of Northumbria University Law School and her PhD student, Aaron Amankwaa. Carole is an acknowledged expert in this area, having been project manager for the Nuffield Council on Bioethics report 'The Forensic Uses of Bioinformation: Ethical Issues' and the Nuffield Foundation project 'The Future of Forensic Bioinformation'. Discussions with her have been invaluable. All four also assisted with comments on a late draft of the report and recommendations.

We are also grateful to the Biometrics and Forensics Ethics Group[3], the body which provides advice to the Home Office in this area. They provided us with a draft paper which formed the basis for much of Chapter 5. They also allowed me to participate in one of their meetings and commented on a late draft of this report.

Special mention should also be made of the contribution of Police Scotland and the Scottish Police Authority. Both organisations offered considerable assistance to our work. Both were represented on the Advisory Group by their Forensic leads. In addition, several others within these organisations assisted us with information whenever requested, especially Calum Dundas, Forensic Data Manager at National Systems Support within Police Scotland. Calum guided us through current systems and procedures, as well as assisting with thoughts about possible future developments. He also commented on late drafts of the report.

A detailed list of meetings and conference calls appears in Appendix 2. All of this assisted us in arriving at our recommendations.

Although all Group members have contributed to the final report, I should make specific mention of Brian Plastow, who produced the original draft of Chapter 2; Diego Quiroz, who drafted the paper which forms the basis for most of the Human

---

[1] https://www.gov.uk/government/organisations/biometrics-commissioner - the Biometrics Commissioner is independent of government. His role is to keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints; decide applications by the police to retain DNA profiles and fingerprints; review national security determinations which are made or renewed by the police in connection with the retention of DNA profiles and fingerprints; provide reports to the Home Secretary about the carrying out of his functions.

[2] https://www.gov.uk/government/organisations/forensic-science-regulator - the Forensic Science Regulator (England and Wales) ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards.

[3] https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group - The Biometrics and Forensics Ethics Group provides independent ethical advice to Home Office ministers on issues related to the use of biometrics and forensics. It is sponsored by the Home Office.

Rights section of Chapter 4; and Ken Macdonald who drafted the Data Protection section of Chapter 4.

Professor Dame Sue Black provided us with helpful suggestions at the start of our work and commented on a late draft of this report. We are very grateful to her.

We also wish to record our thanks to Lindsay MacDougall and, latterly, Ruth Winkler of the Police Strategy and Performance Unit within the Scottish Government, who provided the secretariat for the IAG.

Finding a suitable legislative slot is a constant demand on Government. To this end, we suggest that further work might usefully be carried out in anticipation of legislation following on from our recommendations. We suggest that further development work should take place ahead of public consultation. This work can help to shape the terms of the public consultation, as well as developing the detail of our recommendations, specifically the role of the Commissioner and Ethics Advisory Group, as well as the terms of any legislation and draft Code of Practice.

John Scott QC Solicitor Advocate

7 February 2018

Executive Summary

Biometric data – primarily fingerprints and DNA, although with other technologies developing – are used in the criminal justice process in a number of ways.

Looking specifically at DNA evidence, in the three decades or so that DNA profiling has been in use it has revolutionised the investigation of crime. It is used daily in the investigation of a wide range of offences to identify offenders from minuscule amounts of body fluids and tissues. In sexual offences, DNA profiling can untangle complex mixtures of body fluids, typically found in such cases, to provide evidence that was previously unavailable. The introduction of DNA 24 technology and interpretation software in Scotland is thought to have proved invaluable. The creation of national DNA databases enables the linking of offences where a suspect has yet to be arrested, and the rapid identification of such individuals when they are arrested.

While it is often impossible to say what role such evidence has played in the resolution of particular criminal investigations, there seems little doubt of its significance. Reporting of a recently concluded case in Scotland involving serious organised crime suggests the possible importance of advances in such technologies[4].

Crucially, and often overlooked, DNA evidence is routinely used to eliminate individuals suspected of being offenders.

Both of these uses of biometric data, assisting with identification and elimination, can contribute to public protection.

Finally, DNA profiling plays a critical role in the identification of body parts and tissues, for example in terrorist incidents and civil disasters.

On the other hand, there are concerns about the capture, storage, retention, use and disposal of biometric data in databases within the justice system and elsewhere. These are discussed in more detail elsewhere in the report.

Public confidence in the use of such data is important because of the potential significance of biometric data in individual cases and the justice system as a whole. Such data are a common feature in the most serious criminal investigations and contribute to the overall efficacy of our system of criminal justice, albeit in a way which is unquantifiable. The significance of what can be gleaned from such data, particularly the limitations, is not widely understood. Biometric data has implications for privacy and other fundamental human rights. It is an area which has been explored before in Scotland, but the Scottish Government considered that it should be subject to further review.

---

[4] http://www.bbc.co.uk/news/uk-scotland-glasgow-west-42323466

This report offers a review of evidence relating to the acquisition, retention, use and disposal of biometric data (including DNA, fingerprints and image data) by Police Scotland and the Scottish Police Authority[5] ('SPA'). (See Chapter 1 below for an explanation of the phrase 'biometric data' for the purposes of this report). The report was prepared by an Independent Advisory Group ('IAG'), set up by the Scottish Government at the request of the Cabinet Secretary for Justice in June 2017. Membership of the IAG can be found at Appendix 1. The Terms of Reference are:

To consider the recommendations contained in the HMICS report 'Audit and Assurance Review of the Use of the Facial Search Functionality within the UK Police National Database (PND) by Police Scotland' and:

- advise Scottish Ministers on a policy and legislative framework for the use of biometric data (including facial images and other forms of emerging biometric data) for: the investigation and prevention of crime; public protection; and maintaining public confidence in the use of such data in Scotland;

- advise Scottish Ministers on proposals to strengthen the governance and oversight of the use of biometric data and associated technologies in Scotland, including consideration of whether a Scottish Biometrics Commissioner is required;

- advise Scottish Ministers on the need for, and potential content of, a Code of Practice for the use of biometric data in Scotland;

- advise Scottish Ministers of human rights and ethical considerations in relation to the use of biometric data for law enforcement purposes; and

- advise Scottish Ministers of the general principles that should apply to the use of biometric data for law enforcement purposes.

There has been previous relevant work in this field which has informed our review.

On 27 January 2016, HMICS published the report 'Audit and Assurance Review of the Use of the Facial Search Functionality within the UK Police National Database (PND) by Police Scotland'[6]. That report followed Parliamentary consideration of the issue, especially the retention of custody images[7] of individuals who had been charged but not convicted of a crime. This is an area of particular concern because it is not currently governed by legislation and, in practice, different retention periods and policies apply to the same images when kept on different police databases. The HMICS Report made several recommendations with a view to improving consistency

[5] The Scottish Police Authority is responsible, inter alia, for providing forensic services to support operational policing in Scotland.

[6] https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national

[7] Custody image – photograph of an individual taken when processed at a police office as a suspect or accused person.

and addressing concerns around custody images. The IAG was established, in part, to take forward some of those recommendations.

The issue of biometric data had been considered before in Scotland. Jim Fraser, Professor of Forensic Science at Strathclyde University, reported on the topic in 2008 ('the Fraser Report'), again at the request of the Scottish Government. His review concerned the acquisition and retention of fingerprints and DNA. The Government consulted on his report and some of his recommendations formed the basis of the legislation which now regulates the retention of fingerprints and DNA.

The Scottish statutory regime for fingerprints and DNA was the subject of judicial approval by the Grand Chamber of the European Court of Human Rights in the leading UK case of *S and Marper v the UK* in 2008[8]. Matters have moved on in a number of respects since 2008, in terms of biometric technology as well as jurisprudence, and they may develop further in the next short number of years. We have sought to capture these developments and reflect them in our recommendations.

The first question in our Terms of Reference, as to whether there should be a legislative framework for the use[9] of biometric data, was the simplest to answer. All Advisory Group members agreed that this was not only desirable but necessary, in order to satisfy the obvious requirement of lawfulness for such activity. This aspect was also mentioned by the individuals and bodies who made submissions to the IAG. All who expressed a view stated that legislation is necessary. No one expressed any contrary view.

It is clear from case law in England that legislation is required to govern the retention of custody images – it should be noted that the relevant authority is a High Court decision from 2012[10] and there is still no legislation in England. The issue has not yet been the subject of judicial consideration in Scotland, but it is certain that the English position would be considered by the courts here and there is no reason to anticipate a different approach.

Coincidentally, the period of our review saw a campaign in England and Wales by Big Brother Watch. The campaign is called 'Face Off' and its aim is to 'end the retention of innocent people's custody images.'[11] This coincides with the main focus of concern in Scotland, namely the treatment of biometric data of those who have not been convicted of any offence. In the course of our discussions, we came also to consider wider issues of proportionality and necessity, even in relation to the

---

[8] Applications nos. 30562/04 and 30566/04.

[9] "Use" in the Terms of Reference includes capture, storage, retention, use and disposal.

[10] 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 [2012] EWHC 1681 (Admin)

[11] https://bigbrotherwatch.org.uk/all-campaigns/face-off/.

retention of biometric data of those who have been convicted of criminal offences, where there is currently no minimum threshold of gravity or evidence-based justification for indefinite retention. We gave particular attention to these issues as they affect children.

In our discussions, we considered the question of independent oversight and scrutiny. This is an area which was mentioned in recommendations by Professor Fraser in his report almost 10 years ago. It was also mentioned specifically in the HMICS Report. To date, there is no independent regulator of devolved aspects in Scotland in this area. Those involved in this field in Police Scotland and the SPA appear to work to very high standards of international repute, with a good grasp of the ethical and human rights implications of their work, but that does not obviate the need for independent oversight. The wide-ranging and sensitive information about individuals which can be gleaned from biometric data requires separate and independent oversight with ethical input. The Government's desire to address this is welcome, as it seems likely that we have not yet reached the limits of the potential of biometric technologies.

Accordingly, we recommend that there be legislation to establish a Scottish Biometrics Commissioner ('the Commissioner'). We see the Commissioner overseeing the constantly developing area of biometrics and biometric data in relation to policing and criminal justice (the areas specifically within our Terms of Reference). This is an area which is sufficiently important to justify a Commissioner even if that was the limit of the role. There may be scope for the Commissioner overseeing aspects of biometrics and biometric data in other areas of Government where they feature, for example, health and education, and the private sector, although any such extension is beyond our Terms of Reference.

The question of legislation overlapped with discussions about a Code of Practice. There are, of course, different possible solutions to address the question of lawfulness – legislation alone, a suitable Code of Practice, or a combination of both. There is an attraction in the last of these, especially as we decided to recommend regular review of arrangements under the new oversight regime. As we recommend review of the Code by the Scottish Parliament and the Commissioner, it appears to us to be unnecessary to include every aspect of regulation in the legislation. Having some of the rules and procedures in a Code of Practice, which is itself kept under review, allows for the sort of flexibility which may be necessary in an area where advances in the relevant science and technology can occur quickly. We consider it crucial for rules and oversight to anticipate, or at least keep pace with, technological and other developments. Ideally, to allow this to happen, the Commissioner would work with those who are improving existing technology or developing new technology.

We have specified those aspects of governance which we think should be in legislation and made some suggestions for an outline Code of Practice. We have identified key principles and human rights considerations which might usefully feature in a Code and could be included in public consultation. Further work should be done at an early stage to produce a fuller draft Code for the purposes of public

consultation. The Code can be finalised to come into force when the Commissioner takes office and can thereafter be monitored by the Commissioner and reviewed by the Parliament. In due course, the Commissioner can assess whether a single Code will suffice, or, as it may have various possible audiences – including the public, police, forensic practitioners and private bodies – whether separate Codes of Practice are required for specific and distinct purposes. In looking at this question, the Commissioner can consider not only the different audiences but also any specific requirements for the use of different types of biometric data.

In passing, it should be noted that biometric data may also be retained for reserved matters, notably under national security determinations[12]. Oversight is provided in reserved matters by the UK Biometrics Commissioner, although he has no role in devolved matters. We expect that the Commissioner would work with the UK Biometrics Commissioner in areas of mutual interest. While different legal frameworks apply in Scotland, the ethical and human rights considerations are universal.

Subject to appropriate arrangements for the independence of the Commissioner, the question of precisely where to locate the new regulator is a matter for Government, subject to considerations of public service reform. Some of the options can be included in public consultation. We discuss this later.

We see the Commissioner assisting with public awareness and confidence, although there is a role in this too for Government and others. Ultimately, the public will have a number of choices to make about the type of society in which they wish to live. There is always a balance to be struck between, on the one hand, considerations of public protection and, on the other, the right to privacy and other relevant human rights and ethical considerations. It can be difficult to have a rational debate in the aftermath of specific news stories which may emphasise only one part of the argument. There needs to be a wider debate about the various implications of the capture or surrender of biometric data, especially in terms of the implications for privacy. Privacy is not an infinite commodity. In one of the most frequently quoted statements about the right to privacy, in their influential 1890 article, Warren and Brandeis said[13]:

> ‘Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‘to be let alone’. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’ For years there has been a feeling that the law must

[12] Criminal Procedure (Scotland) Act 1995, section 18G.
[13] Warren and Brandeis, “The Right to Privacy”, Harvard Law Review (1890), Vol.4, No. 5, at page 193.

> afford some remedy for the unauthorized circulation of portraits of private persons… The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.
>
> The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.'

This statement comes from the late 19th century, since which time matters have moved on considerably, albeit the principles and threats are similar. Biometric data, with its greater potential to encroach on the 'inviolate personality', represents a significant challenge to those who wish to preserve 'some retreat from the world.' The circumstances we are discussing involve, primarily, individuals who are convicted of criminal offences, albeit some who are merely accused but not convicted. The fact of an offence, or at least an allegation proceeded with to some extent, provides the current justification for encroachment into privacy.

The principles of proportionality and necessity suggest that we should be careful about the limits of the encroachment we excuse on that basis. This suggests the need to consider and produce a Privacy (or Data Protection) Impact Assessment to support any legislative requirements. Opportunities for engagement on the development of these could be explored with the Information Commissioners Office whose responsibilities are relevant in this area. We will explore this later in the report.

KEY RECOMMENDATIONS

Recommendation 1

There should be national debate to improve public understanding of, and confidence in, the retention and use of biometric data in Scotland for policing, law enforcement and other public protection purposes. Ideally, this should start before and continue during the Scottish Government's public consultation, as well as featuring in ongoing discussion after consultation.

Recommendation 2

Legislation should establish a Code of Practice covering the acquisition, retention, use and disposal of DNA, fingerprints, facial and other photographic images (including custody images) and all existing, emerging and future biometrics for Police Scotland, the Scottish Police Authority and other bodies working in the field of law enforcement. The legislation should outline matters relating to review of the Code by the Scottish Parliament.

Recommendation 3

The Code of Practice should be the subject of detailed consultation. It should contain relevant human rights and ethical principles, address the implications of any presumption regarding retention and specify relevant procedures for applications from private citizens for deletion of biometric data. It should contain specific reference to validation of biometric technologies.

Recommendation 4

Distinct policies should be formulated for the acquisition, retention, use and disposal of the biometric data of children aged between 12 and 17. In each case involving a child, consideration should be given to the proportionality and necessity of obtaining biometric data for the purposes of recording on the biometric databases, ensuring that the best interests of the individual child are taken into account in the decision-making process. Where the decision is to obtain and retain biometric data, the reasons should be recorded and subject to review and scrutiny. Appropriate consideration should be given, and adaptation made, in the treatment of the data of those (children and adults) with specific vulnerabilities.

Recommendation 5

There should be a review of the rules on retention of biometric data in sections 18 to 19C[14] of the Criminal Procedure (Scotland) Act 1995, considering all questions of proportionality and necessity. The review should be research led and consider not only the gravity of the offending but also the value of biometrics in the investigation

[14] With the exception of section 18G which relates to reserved matters.

of certain offences, re-offending rates relating to different crimes, the escalation of offending, and the value that biometric retention has in the investigation of this escalation. It should be informed by any developments in the law in Scotland, England and the European Court of Human Rights.

Recommendation 6

There should be a presumption of deletion of biometric data after the expiry of prescribed minimum retention periods.

Recommendation 7

Evidence should be gathered from which continuing assessment can be made about appropriate periods of retention of biometric data. Public consultation should include specific questions on retention periods.

Recommendation 8

There should be legislation to create an independent Scottish Biometrics Commissioner. The Commissioner should be answerable to the Scottish Parliament, and report to the Parliament. The Commissioner should keep under review the acquisition, retention, use and disposal of all biometric data by the police, SPA and other public bodies. The Commissioner should promote good practice amongst relevant public and private bodies, and monitor compliance with the Code of Practice.

Recommendation 9

An ethics advisory group should be established as part of the oversight arrangements. This group should work with the Commissioner and others to promote ethical considerations in the acquisition, retention, use and disposal of biometric technologies and biometric data.

1 Definitions – Biometrics and Biometric Data

1.1 The term ‘biometric data’ is not defined in existing criminal justice legislation in Scotland. The terms ‘biometrics’ and ‘forensics’ are sometimes (wrongly) used interchangeably.

1.2 There are different definitions and explanations of biometric data, often derived from the relevant technology or specific use of the data. In a policing and criminal justice context, such data can be used to assist in identification of individuals for a variety of purposes – exclusion, incrimination and simple identification of unknown persons. The reliability of such assistance can vary considerably, depending on different factors, including the type of data, the methodology or technology used and the purpose of data collection.

1.3 Regulation of such data should also apply to samples or material from which data can be obtained. We have heard concerns about this area being overlooked through a focus on processing and data. This is subject to the need to retain evidential samples of biometric material for the purposes of an investigation. Such material, sometimes referred to as ‘crime samples’, and associated profiles, is not kept on a database and is retained for as long as a criminal investigation remains open. Our report does not cover this material.

1.4 Biometric data can be produced from many different sources, whether personal, for example, fingerprints and blood, or technological, for example, CCTV footage or images from body worn cameras.

1.5 It may have been simpler if we had felt able to adopt an existing definition, but we wanted to ensure that we captured the widest extent of police and related activity in biometrics, especially as it is a fast-developing area. As new science and technologies emerge, it seems likely that there will continue to be an increase in sources of biometric data. We were also concerned that some existing definitions appear to exclude even obvious biometric data such as DNA profiles.

1.6 For our purposes, we settled on a brief and simple definition. It is intended to include all known biometric data and should be capable of encompassing existing, emerging and future biometric data[15].

[15] Data – ‘information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer', Cambridge English Dictionary.

Definition

1.7 ‘Biometric data are any physical, biological, physiological or behavioural data, derived from human subjects, which have the potential to identify an individual.’

2 Current Landscape – Scotland

2.1 This Chapter explains the current legislative framework, policy and operational practice relevant to the acquisition, retention, use and disposal of biometric data by Police Scotland and the Scottish Police Authority as part of the criminal justice process in Scotland.

2.2 In doing so, the Chapter draws on key findings from the 2016 HMICS Audit and Assurance Review of the facial search functionality within the UK Police National Database (PND), and the recommendations from that report to Scottish Government which in turn formed the basis for the terms of reference for the IAG on Biometric Data[16].

2.3 Those terms of reference have a specific focus on biometric data used for the investigation and prevention of crime; public protection; and maintaining public confidence in the use of such data. Accordingly, this Chapter primarily explores the current landscape in the most commonly used forms of biometric data collected for law enforcement purposes (DNA, fingerprints and photographic images taken as part of the criminal justice and custody process). This includes current information on the number of biometric data records of varying types held by Police Scotland and the SPA.

2.4 Reflection on the current landscape highlights various human rights and ethical considerations in the use of biometric data for law enforcement purposes and, in turn, emphasises the need for strengthened governance and independent oversight. This includes opportunities, as highlighted by HMICS, to close a specific legislative gap in Scotland relating to the acquisition of custody images by the police, and to introduce background context on matters that will be discussed later in this report, such as questions about the proportionality, effectiveness and efficiency of current biometric data retention regimes.

2.5 Although the IAG terms of reference called for a primary focus on law enforcement in Scotland, there is also a range of other public agencies in Scotland that collect biometric data from citizens in varying circumstances and for differing purposes. Additionally, biometric image capture technologies are increasingly sourced from the private sector. This results in a gap in scope for independent evaluation of the effectiveness of technologies whose biometric identification algorithms[17] are protected by issues of commercial confidentiality. These issues were also highlighted

[16] https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national.

[17] Algorithm – 'A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer', Oxford Dictionaries.

by HMICS which noted, for example, that there had been no operational evaluation of the effectiveness of the facial search functionality within the Home Office UK Police National Database (PND)[18]. Accordingly, these other areas are introduced briefly in the current Chapter, solely to assist in identifying opportunities to strengthen governance and oversight over biometric data collection and use in Scotland.

2.6 The Chapter also engages throughout with the issue of interoperability requirements for biometric databases used in sector-specific contexts, and particularly in relation to law enforcement. Such connectivity and exchange between biometric databases is a particularly important area for policing as Scottish data are aggregated to UK biometric databases maintained by the Home Office, which in turn gives Scottish policing access to biometric data from other jurisdictions. This national and international interoperability is vital in the wider interests of UK national security. Properly regulated interoperability will ensure that human rights considerations are not overlooked. We have also considered, as far as possible, potential alignment to the anticipated policy objectives of the Home Office Biometrics Strategy currently under development as part of the Home Office Biometrics (HOB) Programme.

Statutory Framework for Criminal Justice biometric samples in Scotland

2.7 The Criminal Procedure (Scotland) Act 1995 ('the 1995 Act') is the primary Scottish legislation allowing the retention of fingerprints and other biometric samples from a person arrested by the police. Sections 18 to 19C stipulate the conditions under which samples may be taken by the police, as well as rules for retention and specification of the purposes of use of samples[19].

2.8 Section 18 (2) states: 'A Constable may take from the person, or require the person to provide him with, such relevant physical data as the Constable may, having regard to the circumstances of the suspected offence in respect of which the person has been arrested, reasonably consider it appropriate to take from him or require him to provide, and the person so required shall comply with that requirement'.

2.9 The 1995 Act does not refer to facial images. It defines 'relevant physical data' as 'a fingerprint, palm print, print or impression of an external part of the body or record of a person's skin on an external part of the body created by a device approved by the Secretary of State'[20]. However, the term biometric data is usually thought to include

[18] Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND), Paragraph 67, HMICS: January 2016: https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national.
[19] Criminal Procedure (Scotland) Act, 1995: https://www.legislation.gov.uk/ukpga/1995/46/part/II/crossheading/prints-and-samples
[20] Criminal Procedure (Scotland) Act, 1995, s 18(1)(7A).

facial images[21]. The absence of legislation in Scotland giving explicit authority to the police to take custody episode photographs is at variance with specific legislative authority in other parts of the UK. This was identified in the HMICS Audit and Assurance Review in 2016 and led to a specific recommendation for the Scottish Government to consider legislative provision in relation to the retention and use of photographic images by the police[22].

2.10 Section 83 of the Police, Public Order and Criminal Justice (Scotland) Act 2006 inserted Section 18A into the 1995 Act and contains provisions to allow retention of DNA samples and profiles of persons who have been arrested but not convicted of certain sexual or violent crimes. The list of relevant sexual and violent offences is in section 19A(6) of the Act[23].

2.11 In 2010, as part of the response to the Fraser Report, the Scottish Government also introduced sections 77 to 82 of the Criminal Justice and Licensing (Scotland) Act 2010 which included provisions to develop the law in relation to the retention and use of DNA, fingerprints and other physical data. This was done by amendment to the 1995 Act.

2.12 In brief terms, the statutory framework in Scotland for the retention of fingerprints and DNA biometrics is as follows:

- Fingerprints and DNA data from convicted individuals can be retained indefinitely[24]. This policy applies to adults and children[25] on the basis of a single criminal conviction for any type of offence, regardless of gravity;
- Data from children dealt with at the Children's Hearings system may be retained only where grounds of referral are established (whether through acceptance by the child at such a hearing or a finding at court) in relation to a prescribed sexual or violent offence. Such data can only be retained for three

[21] Biometrics Commissioner: Oral Evidence to House of Commons Science and Technology Committee on current and future uses of biometric technologies, 10 December 2014.
[22] Recommendation No 1: Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND), HMICS: January 2016: https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national
[23] Inserted by section 48 of the Crime and Punishment (Scotland) Act 1997.
[24] Although indefinite retention is legally permissible, in practice the technical process of retaining fingerprints on the national IDENT1 database is dependent on the retention of the associated conviction on the individual's criminal record. Therefore, once the conviction weeds from the Criminal History System (retention periods: http://www.scotland.police.uk/assets/pdf/340047/341626/recording-weeding-and-retention-of-information-on-criminal-history-system-chs?view=Standard) electronic and hard copy records of the fingerprints taken for that case will be destroyed by the SPA.

[25] Only a very small number of children aged under 16 are convicted at court as opposed to appearing in the Children's Hearings system.

years unless the police apply for, and are granted, an extension by a Sheriff. For less serious offences, and where grounds are not established, there is no retention in relation to children;

- Data from individuals who accept a Fiscal Offer[26] may be retained for three years in relation to a prescribed sexual or violent offence, with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of a particular person's data); and data may be retained for two years in relation to non-sexual or non-violent offences which are the subject of a Fiscal offer or fixed penalty notice from the police;
- Data from individuals prosecuted for certain sexual and violent offences may be retained for three years (whether or not they are convicted), with the Chief Constable able to apply to the Sheriff Court for further two year extensions (there is no limit on the number of two year extensions that can be granted in respect of a particular person's data)[27]; and
- Subject to the exception just stated, data from individuals arrested for any offences (and who have no previous convictions) must be destroyed immediately if they are not convicted or if they are given an absolute discharge.

2.13 Whilst it has been custom and practice in Scotland for over 100 years for the police to take photographic custody images of persons who have been arrested or detained, there is no specific legislation, Scottish or UK, which gives powers to Police Scotland to take such images. There is no legislation which specifically regulates the retention periods for such images, or indeed the way in which such images may be used. This means the Scottish legislation around biometric data retention by the police centres primarily on fingerprints and DNA data and not on data from photographic images[28].

2.14 Before examining retention periods in more detail, it is useful to summarise briefly the main biometric data record types held by the police and other law enforcement agencies, and to reflect on the purposes for which such data are used.

---

[26] Fiscal offer – offers made by the Procurator Fiscal in terms of the 1995 Act: a conditional offer of fixed penalty under section 302; a compensation offer under section 302A; a combined offer (fixed penalty and compensation offer) under section 302B; a work offer (number of hours of unpaid work) under section 303ZA.

[27] At the time of writing, Police Scotland has not made any application to further retain data relating to a person prosecuted but not convicted of certain sexual and violent offences. Source: Police Scotland IAG representative.

[28] It should be noted that Section 87(4) of the Sexual Offences Act 2003, which relates to the sex offender registration process, gives the power to the police take photographs and fingerprints of the subject for this specific purpose.

DNA in the Criminal Justice Process

2.15 DNA is Deoxyribonucleic Acid. This is the genetic material which can be found, although not exclusively, in the nucleus[29] (centre) of most cells in the body. It contains a person's genetic information – it is a genetic 'code' unique to each of us. We inherit 50% of this DNA from our mother and 50% from our father. Our DNA determines the colour of our eyes, our hair colour and many other physical characteristics. The DNA in a person's body is the same regardless of which body fluid or cell type it comes from. It is therefore possible to create a DNA profile from samples such as blood, saliva, semen, hair roots, etc.

2.16 In forensic science, the process of analysing DNA is referred to as DNA profiling and involves targeting specific parts within the DNA known as Short Tandem Repeats (STRs). DNA profiling in Scotland looks at 24 areas of a person's DNA – a significant step up from the 11 areas that made up previous DNA profiling technology and an advance on the 17 areas which is the European standard[30]. These 24 areas do not code for any known characteristic like eye colour. This technology makes it possible to compare a DNA profile from a person, known as a reference sample, with a DNA profile from a 'crime' sample, for example, from the scene of a known crime. If there is a match between the DNA profile from the person and that of the crime sample, it can be stated in terms of probability. For example, if a good quality DNA sample is found, a probability of 1 in more than 1 billion of such a match if the DNA came from a male unrelated to this person. This is why DNA has become so important in criminal investigations as it can be used to exclude an individual as a source of DNA or to contribute to proving guilt.

2.17 DNA was first used in criminal investigation in the UK in the 1980s following a double rape and murder in Leicestershire. This led to the production of the first DNA profile which showed that both murders had been carried out by the same individual, who was not the prime suspect. Leicestershire Constabulary then carried out the world's first DNA intelligence-led screening. All adult males in three villages – a total of 5,000 men – were asked to volunteer and provide blood or saliva samples. A local baker, Colin Pitchfork, was arrested, and his DNA profile matched with the semen from both murders. In 1988 he was sentenced to life imprisonment for the two murders.

2.18 The Scottish DNA Database is held in Dundee. When a suspect is arrested, the police have the right to take a DNA sample, usually a mouth swab. This is known as a criminal justice sample. All samples are analysed by the SPA, and the profiles are stored on the Scottish database as well as being sent to the National DNA Database, set up in 1995 and based in Birmingham. The Scottish DNA Database is

[29] Commonly referred to as nuclear DNA as distinct from other forms of DNA found in other parts of cells such as mitochondrial DNA. The National DNA Database is a repository of nuclear DNA data.
[30] http://www.spa.police.uk/news/322981/296781/

administered by the National Systems Support department of Police Scotland. DNA profiling from samples taken from subjects and crime scenes is undertaken by the SPA Forensic Services. All profiles on the Scottish DNA Database are exported to the National DNA Database which gives all police forces throughout the UK the ability to search for profile and crime scene matches. The exception to this is profiles taken from volunteers for the purpose of intelligence led screens. These samples are only compared against the crime scene profile in question and destroyed on conclusion of the investigation or, subject to any evidential requirement, if the volunteer withdraws their consent to retention.

2.19 The DNA sections of the SPA provide four key services to Police Scotland and other law enforcement agencies. Those are:

- Casework – These are cases where there is a known accused and comparisons can be made between reference samples and a crime sample.
- Undetected cases – These are where the police do not have a suspect and where the Scottish DNA database and UK National DNA Database are used to try to identify matches between a crime sample DNA profile and the profile of a person held on the database.
- Criminal paternity testing – in cases of rapes and incest etc.
- Identification of individuals – missing persons, bodies and body parts.

2.20 The SPA publishes monthly DNA Database statistics on its website, including the number of profiles held, added or removed. This data includes information on crime scene matches and information on data held by age and gender. As at the end of December 2017, there were **332,213** criminal justice samples (not including crime scene samples) retained on the Scottish DNA Database[31]. A process map showing the Scottish DNA Database process from crime scene to conviction is attached to this report (Appendix 6**).**

Fingerprints in the Criminal Justice Process

2.21 The system of identification using fingerprints rests upon three fundamentals – the formation, uniqueness and persistence of the highly distinctive ridge patterns found on fingers (and some other parts of the body). Fingerprints develop early in foetal life before birth. Pads (bumps) form on fingers between weeks six and thirteen. Where these pads occur, how the baby moves around inside the womb and how fast and big the baby grows all affect how the fingerprint patterns and ridges form and ensure the apparently unique properties of fingerprints are never duplicated. The details of a person's prints are considered unique to them. Identical twins do not have identical fingerprints. This is why fingerprints are a generally reliable means of identification at all stages of a person's life.

[31] Scottish Police Authority website accessed 07 December 2017: http://www.spa.police.uk/assets/151078/427288.

2.22 The impression left by the owner of the fingerprints at a crime is referred to as a ‘mark' or fingermark. A ‘print’ is the sample taken from an individual by the police for identification purposes. This is normally a set from the five digits on each hand, referred to as ‘tenprints'. Tenprints are the rolled impressions made on a fingerprint form taken under controlled conditions, normally at a police office. Tenprint forms are initially searched against other tenprint forms held on the national fingerprint database to establish if the individual already has a criminal record for previous offences or is new to the system. The searching of the tenprint form against other tenprint forms allows for confirmation of identity and accuracy of information supplied by the arrestee along with the accurate alignment of offences to an individual’s criminal record or the generation of a new criminal record when required. These searches are completed in real time with a result returned to the relevant custody location within two hours from time of electronic submission of a set of tenprints. When marks are submitted from a crime scene these are assessed by fingerprint examiners for suitability for further examination. The mark is then compared against specific individuals whose names have been submitted by the investigating officer/Procurator Fiscal and can be speculatively searched against the national fingerprint database to establish if the mark has been left at the crime scene by an individual already on record with previous convictions.

2.23 Scottish fingerprints are uploaded to IDENT1 which is the UK central national database for holding, searching and comparing biometric data on those who come into contact with the police as detainees after being arrested. Information held includes fingerprints, palm prints and scenes of crime marks. IDENT1 currently contains the fingerprints of more than 7 million people and makes 85,000 matches with data recovered from crime scenes each year.

2.24 The SPA does not publish fingerprint data on its website due to the Scottish information being hosted directly on the UK Home Office System. However, in August 2017 it is known that the SPA and Police Scotland held fingerprint records for **432,888** people[32]. This number reflects current long-term retention policies and includes records for non-residents.

[32] Source: Data provided by Police Scotland on 21 August 2017 in response to Freedom of Information request.

Criminal History System (CHS) photographs in the Criminal Justice Process

2.25 Police Scotland maintains a Criminal History System (CHS), where all records and images of charged and convicted persons are stored. The criminal history images within these records are derived from photographic images relating to a particular custody episode when an arrested[33] person is brought into police custody.

2.26 As indicated in the 2016 HMICS Audit and Assurance review, the criminal history records and images of persons charged with, or convicted of, a common law crime or statutory offence in Scotland on CHS are uploaded automatically to a UK policing intelligence sharing system known as the Police National Database (PND), so that other UK forces can search the PND to help identify and prosecute criminals. In the event of acquittal, the Scottish records and images are removed from CHS and PND by Police Scotland once notified of non-conviction or absolute discharge by the Crown Office and Procurator Fiscal Service (COPFS). If a child is referred to the Children's Hearings system, images are destroyed.

2.27 Although the 1995 Act does not provide specific legal authority in relation to photographic images, Police Scotland voluntarily applies a similar policy to the retention and weeding of photographs on CHS as exists in primary Scottish legislation for fingerprints and DNA. This means that images of persons not subsequently convicted (and who have no previous conviction) are removed from CHS and PND by Police Scotland in no proceedings/non-conviction scenarios, subject of course to the three year retention periods permitted for certain sexual and violent offences as defined in Section 48 of the Crime and Punishment (Scotland) Act 1997. This was acknowledged as effective practice by HMICS in 2016 and contrasted favourably with the position in other parts of the UK where many forces in England and Wales have been criticised by the UK Biometrics Commissioner for retaining custody images of innocent people on the Police National Database (PND) despite the 2012 ruling by the High Court in England that this was unlawful[34].

2.28 In August 2017, Police Scotland held **633,747 CHS photographs** of 362,348 different people. This number reflects current long-term retention policies and includes records for non-residents. Unlike DNA and fingerprints, the physical appearance of a person will change over time, through ageing, injury or otherwise, and indeed is sometimes changed intentionally in an attempt to evade identification and detection. This is why the police will often hold multiple images of offenders who have multiple criminal convictions. A process map showing the Police Scotland and

---

[33] Also includes images from those detained before detention was abolished by the Criminal Justice (Scotland) Act 2016.

[34] Annual Report 2015: Biometrics Commissioner, Chapter 7, Custody Photographs and Facial Recognition Technology. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/507105/54496_Biometrics_Commissioners_Web_Accessible.pdf

SPA biometric retention process is attached to this report (Appendix 7). It should be noted that this Police Scotland process map is intended as a guide only. It does not illustrate the process for custody images and does not fully illustrate indefinite retention on the basis of a single conviction.

Custody episode images

2.29 Whenever a person is detained or arrested by the police and is brought into the custody environment, a computerised record is created. Included within each record is at least one digital image/photograph of the subject. A CHS image is only created after a person has been cautioned and charged with a relevant offence. It is also at this point that other criminal justice samples such as DNA and fingerprints are taken.

2.30 Police custody images in Scotland are only uploaded to CHS and PND if the subject has been charged with a crime or offence. This differs from the position in England and Wales where most forces upload all custody images directly to PND due to the absence of images on the Police National Computer (PNC) (the PNC holds a reference to the image held locally within each force) or any statutory controls or guidance to the contrary.

2.31 At the time of the HMICS report in 2016, there was no national custody software solution in place in Scotland and Police Scotland were retaining custody images on the different legacy custody applications of the eight former police forces. It was also noted by HMICS that Police Scotland did not have weeding policies in place to cater for the timely disposal of the photographic images of persons not subsequently charged or convicted. Instead, such images were, and are, retained by Police Scotland under general data retention policies for a minimum period of one (current year) + six years. This means that photographs of people are routinely retained by Police Scotland for a period of up to seven years, even where they have not been convicted of any offence. This practice contrasts with the approach taken in Scotland for fingerprints, DNA data and the CHS images/photographs which are all destroyed if no proceedings are taken against the person to whom those various biometric records relate, providing that they have no existing criminal convictions.

2.32 Since the publication of the HMICS report in 2016, Police Scotland has rolled out a new national custody solution (completed January 2017) to manage custody episodes in a single and consistent way across Scotland. This solution will result in the records within various legacy custody applications becoming of less relevance. Legacy applications do not afford the same functionality or flexibility to identify and remove custody images of people who are not convicted/not proceeded against. Access to these legacy applications, and therefore the images retained, is limited to geographical areas and certain staff, predominantly dedicated custody staff. A legislatively mandated weeding regime based on the disposal of the associated case would require Police Scotland to consider a policy, process and technical response to ensure compliance within an acceptable timeframe in relation to the legacy custody applications. Although Police Scotland has not yet changed its policies on custody image retention, it has indicated that weeding conventions are capable of

being programmed into the new custody software. This means that Police Scotland should have the technical capability to remove and dispose of the photographs of people who are not convicted/not proceeded against from the new system in a timelier manner, and in a way that is consistent with the existing legal framework in relation to DNA and fingerprints and Police Scotland's own policy relative to the corresponding CHS image derived from the same custody episode. It also offers a greater capacity for compliance with any changes to biometric retention regimes arising from this IAG report.

2.33 Based on a one + six year retention policy, Police Scotland currently holds or retains **more than 1 million custody images**[35]. Police Scotland has no technical means of understanding how many people these records relate to and has no automated means of establishing how many custody images it holds of people who have not been convicted of any offence.

2.34 For ease of presentation, the data from the foregoing paragraphs is summarised in Table 1, below:

Table 1: Summary of biometric data records retained by Police Scotland and the SPA

Biometric Data Type	Number of records held	Comments
DNA Profiles	332,213	
Fingerprints	432,888	
CHS photographs	633,747	These relate to 362,348 individuals.
Custody photographs	1,000,000 +	It is unknown how many of these images relate to persons not charged or convicted of any offence.

2.35 These reflections on the current landscape are intended to introduce questions about the proportionality, effectiveness and efficiency of current biometric data retention regimes in Scotland. Whilst these will be discussed in some detail later in this report, it is apparent from initial review that the absence of specific legislative authority for the police to capture custody episode images raises important human rights concerns. The non-statutory status of some of the biometric retention regimes described above also raises concerns about the lack of sufficient differentiation for the special position of children and vulnerable individuals in our society.

[35] Police Scotland and NHS: National Co-ordinating Network for Healthcare and Forensic Medical Services for People in Police Care, Annual Report 2016-2017: http://www.policecare.scot.nhs.uk/wp-content/uploads/2015/01/Annual-Report-2016-17-v1.0.pdf

2.36 In relation to children, the numbers entering the criminal justice system in Scotland is small by comparison to adults, with Scottish Government data showing around 2,200 criminal proceedings being initiated against persons aged between 12 and under 18 in 2017, the vast majority of whom were aged 16 or 17[36]. This means that biometric data are rarely captured from younger children, and they are likely to be taken from those in their mid-teenage years only in circumstances where the gravity of their offending or other circumstances are likely to result in criminal proceedings.

2.37 In the case of children, such small numbers raise questions about value and utility, as well as allowing for the possibility of introducing a more nuanced and individualised risk-based decision-making model in relation to biometrics acquisition and retention that better balances the needs of law enforcement with the best interests, needs, rights, and life chances of the small numbers of children whose offending brings them into contact with the criminal justice system in Scotland. It also calls into question the proportionality of a 'one size fits all' policy which sanctions indefinite retention of biometrics on the basis of a single criminal conviction for any offence, regardless of seriousness (albeit the number of children involved is very small as most are dealt with by the Children's Hearings system).

2.38 Notwithstanding the broader question of whether there is a need to keep biometric data from children out of aggregated adult biometric databases completely, the available data confirms trends of decreasing criminalisation of children, and correspondingly increasing trends in alternative social policy solutions as part of the Scottish Government Whole System Approach to dealing with children involved in offending[37].

Biometric governance issues previously highlighted in Scotland

2.39 In 2007, the Scottish Government asked Professor Jim Fraser to review the operation and effectiveness of the legislative regime governing police powers in relation to the acquisition, retention, use and disposal of fingerprint and DNA data. He was directed to consider additional powers insofar as they related to the retention of forensic data.

2.40 In 2008, his report was published and made eight recommendations, many of which were implemented in the Criminal Justice and Licensing (Scotland) Act 2010. Two recommendations which were not taken forward into statute were:

a) The current governance arrangements for DNA and fingerprint databases in Scotland should be reviewed as a matter of urgency. Future arrangements should

[36] Scottish Government Progress Report on the Implementation of the Youth Justice Strategy, June 2017: http://www.gov.scot/Publications/2017/06/3198
[37] ibid

take into account good practice in scientific and ethical standards, efficient and effective management and independent oversight.

b) Sufficient information regarding the governance and management of forensic databases should be in the public domain to maintain transparency, accountability and public confidence in their use.

2.41 Recommendation a) remains outstanding. Recommendation b) was addressed to some extent through implementation work following the Fraser report. Scottish Government web pages were developed to provide information to the public and support transparency. As mentioned above, there is also monthly publication of statistics by the SPA. Such information gives the public access to information on how DNA is used in connection with law enforcement in Scotland and gives an indication of its effectiveness in the investigation of crime.

2.42 In 2016, HMICS considered the current governance arrangements in place in Scotland with regard to the use of biometric data by Police Scotland and the SPA. HMICS concluded that whilst it was clear that effective internal governance arrangements were in place between key partners, those arrangements did not deliver the necessary levels of independent oversight as called for in the Fraser Report[38].

2.43 Endorsing the findings in the Fraser Report, HMICS recommended the creation of a Scottish Biometrics Commissioner so that public confidence in the police use of biometrics could be maintained through an independent office reporting to the Scottish Parliament[39]. In making this recommendation, HMICS noted the absence of biometric and forensic regulators in the Scottish context by contrast with other parts of the UK where there is a Biometrics Commissioner, a CCTV Surveillance Camera Commissioner, and a Forensic Science Regulator for England and Wales.

2.44 HMICS concluded that a Scottish Biometrics Commissioner offered the potential to build capacity and resilience in Scotland, and to explore emerging human rights and ethical considerations around the use of biometric data, not only for policing purposes but also by other public agencies involved in the collection and use of biometric data from citizens. In particular, HMICS highlighted public space CCTV systems, Road Camera Enforcement Systems and Automatic Number Plate Recognition Systems (ANPR)[40].

---

[38] Paragraph 49, Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND), HMICS: January 2016: https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national.

[39] *Ibid,* Recommendation No 2.

[40] Ibid, Paragraph 52.

2.45 HMICS also noted the exponential growth of biometric technologies in contemporary society which escalate the value and possibilities around the use of biometric data. It was argued that, when combined with the development of an underpinning Codes of Practice, the creation of a Scottish Biometrics Commissioner could both safeguard and future-proof what will undoubtedly continue to be a fast evolving landscape[41].

2.46 Although the question of independent oversight remains outstanding, it should be noted that in the summer of 2017, the SPA Board took steps to improve scrutiny and governance of forensic services and address some of the recommendations made by the HMICS Inspection of Forensic Services published in June 2017[42]. The Director of Forensic Services, IAG member Tom Nelson, reports directly to the SPA Board and a new Forensic Services Committee[43], chaired by SPA Board Member, Iain Whyte, was established. This committee meets regularly in public.

Biometrics in other public sector contexts

2.47 Whilst this Chapter has focussed primarily on the current biometrics landscape as it relates to the criminal justice context, biometrics capture technologies are in use in a range of other policing and non-policing contexts. In policing, images of citizens can be captured through body worn video cameras or by Public Order Surveillance Teams at demonstrations and events, or through air-based technologies such as helicopters or drones.

2.48 In a non-policing context, there are public space CCTV systems, Road Camera Enforcement Systems and ANPR, all of which can capture the facial images of citizens engaged in routine lawful activity. In education, some schools operate biometric identification systems where the fingerprints of children are captured and used with parental consent. In a health context, a report on Guthrie Cards in Scotland explored the ethical, legal, human rights and social issues surrounding the existence, continued storage, and future uses of the new-born screening collection[44] held in Scotland (also known as the Guthrie Card collection)[45]. The report highlights how such biomedical collections inadvertently operate as a *de facto* DNA database and discusses the various ethical considerations that arise. The report ensured that Guthrie Cards were included in the developing governance regime for biomedical collections within Scotland.

---

[41] Ibid, Paragraph 52.
[42] https://www.hmics.scot/publications/thematic-inspection-scottish-police-authority-forensic-services.
[43] http://www.spa.police.uk/meetings-events/fscom/.
[44] New-born blood spot screening involves taking a blood sample to find out if your baby has one of nine rare but serious health conditions.

[45] Guthrie Cards in Scotland: Ethical, Legal and Social Issues, Social Research Council: 2013

2.49 The relevance of this medical example is that it highlights the ethical dilemmas of collecting biometric data and subsequently using aggregated metadata for purposes for which it was not originally intended. Although set in a medical context, this example highlights the need for biometric samples to be collected and used within an appropriate legal framework so that relevant human rights considerations can be addressed. It also highlights the need for sound governance and accountability mechanisms, including a framework involving independent ethical oversight.

2.50 In a policing context, there are clear parallels to be drawn from the personal biometric data collected from individuals which subsequently become part of aggregated and searchable law enforcement biometric data sets such as those for fingerprints, DNA and photographic images in the Police National Database. There is also increasing availability of open source biometrics, notably those which could be processed using facial recognition technology.

2.51 In addition, and as part of the Scottish Government's Digital Strategy for Justice in Scotland, a digital evidence sharing capability is being developed between criminal justice partners. Subject to successful prototyping, testing, and the securing of future funding, this presents opportunities to transform how evidence, including biometric data, is accessed across the justice system, allowing for more efficient sharing of evidence with consequential benefits which may accompany that development. However, it also presents ethical challenges in relation to the safeguarding of biometric data within the context of a shared multi-agency secure digital platform.

Biometrics – UK Government Strategy

2.52 There has been broad political support at Westminster for the notion of enhancing regulation, governance and independent oversight of the use of biometric technologies, and calls for the development of a Biometrics Strategy by the UK Government:

2.53 ‘In the absence of a biometrics strategy, there has been a worrying lack of Government oversight and regulation of aspects of this field. We were particularly concerned to hear that the police are uploading photographs taken in custody, including images of people not subsequently charged with, or convicted of, a crime, to the Police Database and applying facial recognition software. Although the High Court ruled in 2012 that existing policy concerning the retention of custody photograph by the police was ‘unlawful’, this gap in the legislation has persisted. At the very least, there should be day-to-day, independent oversight of the police use of all biometrics. We therefore recommend that the Biometrics Commissioner’s

jurisdiction should be extended beyond DNA and fingerprints to cover, at a minimum, the police use and retention of facial images'[46].

2.54 Against the context of parliamentary concerns, the UK Government continues to develop a biometric strategy as part of the HOB Programme. It is anticipated that the strategy will be completed in 2018 and will be directed at Home Office functions and areas such as policing, immigration and the justice sector in England and Wales. The HOB Programme includes a privacy and ethics impact assessment committee so that ethical and privacy considerations can be designed in to the new strategy.

2.55 Whilst a key objective of the HOB Strategy will be to deliver greater interoperability between key UK partners, discussion with Home Office officials has also provided clarity for the IAG on matters of reserved and devolved competence. From discussion, it would appear that there is a consistency of thinking and a corresponding golden thread through the work in each jurisdiction which encompasses respect for human rights, ethical standards, compliance with the law, and improving public confidence and trust.

2.56 In concluding discussions on the current landscape, it is clear that we live in an era of ever increasing proliferation of automated biometric identity systems with associated application to law enforcement and other public functions. In this context, it is essential that sensitive personal data are collected only for specific, explicit, lawful and legitimate purposes. In seeking to achieve a careful balance between the needs of citizen and state, there is clearly a need for independent oversight, and for the development of a broad framework of consistent ethical and human rights-respecting principles against which all biometric use for policing, law enforcement and public protection purposes in Scotland can ultimately be checked.

[46] House of Commons, Science and Technology Committee, Sixth Report of Session 2014/15, page 3.

3 Public Awareness and Confidence: Perceived Benefits and Concerns

3.1 In general, there appears to be a lack of knowledge of, and relative lack of interest in, biometrics and biometric data on the part of the public. This is consistent with evidence about public awareness of new technologies more generally.

3.2 There is occasional political and media interest in the subject, with concerns having been expressed, for example, at the Scottish Parliament[47].

3.3 Public views on the use of biometric data in policing, insofar as known, appear to range from supportive to concerned. Much depends on the particular headline which attracts attention: for example, the use of facial recognition technology proved controversial at the Notting Hill Carnival in 2017, with stories of mistaken and unreliable identifications[48]. This is in contrast to the effective and apparently welcome use of such technology in South Wales at the Champions League Final and an Elvis Convention[49].

3.4 Public reaction depends often on the framing and context of any stories and the amount of accompanying information. As well as taking into account the written submissions and other views we received, we have surveyed newspaper reports, social media and articles from which we have compiled these short lists of publicly perceived strengths/benefits and concerns/risks regarding the use of biometric data:

---

[47] 16/03/2015 - Motion S4M-12676: Alison McInnes, North East Scotland, Scottish Liberal Democrats. Police use of Images with Facial Recognition Technology: 'That the Parliament understands that police forces from across the UK have uploaded up to 18 million photographs to the Police National Database for use with facial recognition technology; is concerned that these images might include those of people never
charged with an offence or who have been found innocent of a crime; notes the statement by the Chief Constable of Durham Constabulary on Newsnight on 2 February 2015 that, in a recent case in his constabulary, a person was identified using photographs from Scotland; further notes the concerns of the Biometrics Commissioner, Alastair MacGregor QC, regarding the implications for civil liberties of the use of such technology; notes his comment that "urgent steps" should be taken to ensure that facial recognition and other biometric technologies should be governed by an appropriate regulatory regime; considers that, although facial recognition technology might be a useful policing tool, such technology must only be used with suitable safeguards and protection for innocent members of the public; believes that Police Scotland's use of, or contribution of images to, the Police National Database, or any other database for facial recognition purposes, should be in the context of specific laws set by the Parliament, and considers that legislation similar to that agreed by the Parliament to govern the use of DNA profiles and fingerprints should be adopted to regulate the police use of images for facial recognition purposes and that police use of any new biometric identification technology in the future should be subject to similar regulation'.

[48] https://www.theregister.co.uk/2017/08/31/met_denies_face_recog_wrongful_arrest_carnival/

[49] https://www.facebook.com/SWPolice/posts/1658433710876077.

Perceived strengths/benefits

- Biometric data are a common resource in the criminal investigation process and often provide vital evidence for the purposes of identification or confirmation of a key individual (for example, a suspect or victim) in a police inquiry.
- Biometric data can be used to exclude or eliminate an individual from suspicion in a police inquiry.
- Non-criminal police inquiries use biometric data, such as those that involve tracing a missing person or identifying accident or fire victims.
- The benefits listed above contribute to general protection of life and other human rights.
- The hereditary nature of DNA means that it can be used not only for individual identification but also for the identification of family members (e.g. identifying a body through the DNA of a close relative).
- Routine security of personal data on electronic devices such as phones, laptops.
- The use of biometric data is now a core aspect of modern financial transactions, providing a service that is more secure than prior banking technology (thus preventing fraud and criminality) while at the same time improving accessibility and convenience to the public.
- As a means of maintaining border security.
- There are many legitimate research purposes for biometric data, and new advances in the use and governance of information sharing and data linkage can ensure that the data have wider benefits beyond that of the data itself.

Perceived concerns/risks

- Concerns about security and the ability to steal identity to facilitate fraud/spoofing.
- Concerns about where the biometrics data are stored and who has access.
- Concerns over possible state control and the loss of a right to anonymity.
- DNA phenotyping – the prediction of a particular trait, such as skin colour, according to the individual's genetic makeup.
- Discrimination/prejudice – there is evidence of unconscious bias even in algorithms.
- Lack of transparency in algorithms due to commercial confidentiality.
- Linkage and sharing of different databases with development of a detailed picture of individuals without informed consent.
- Use of data for other than intended purposes.
- Length of retention periods.
- Sharing of data.
- Impact on privacy and other human rights.
- Familial identification – without knowledge/consent.
- Ethical considerations.
- Potential for misidentification or misuse.

- Incorrect assumptions about the effectiveness of biometrics, including the perception that some are infallible.
- Increased securitisation (through security agendas dominating social policy debates) and increase in intrusive measures.
- Stigmatisation.
- Members of the public leave private information about their lives and activities across a wide range of public and private databases, and in public spaces. This allows for multiple ways of checking identity, modelling patterns of social behaviour, collecting or inferring attitudes and recording activities, movements and decisions. Therefore, behavioural or biographic sociometrics (which includes aspects of such modelling and recording) is an area of possible concern. This is a possible development, for example, in the analysis of CCTV footage. There is already some familiarity with simple versions of such analytics, for example when websites offer goods or services tailored to predictions of preferences or needs.

3.5 It will be observed that there is some overlap between perceived benefits and risks, for example, in relation to familial identification. Much depends on context. Well-informed debate should engage with these perceptions which are all valid, at least to some extent. Indeed, this is an area in which the benefits and risks co-exist, with greater public awareness being the key to justified levels of confidence and trust which recognise the advantages as well as the costs. From greater awareness should come an appreciation of some of the ethical considerations, with public support based on reality rather than the latest headline.

3.6 Biometric technologies continue to become an increasing part of everyday life for many, with apparent benefits in terms of fraud prevention, security and maintaining privacy. Think, for example, of mobile phones, passports, banking, schools, shopping, migration, terrorism and CCTV. There is increasing familiarity with such use of biometric data, albeit without much technical understanding, discussion or debate. This limited familiarity can lead to assumptions about reliability of biometric technologies, perhaps even extending to assumptions of certainty or infallibility. Such assumptions are misplaced.

3.7 None of the advances in such technologies leads to absolute certainty. The reliability of any technology will derive from a variety of factors such as its design, including the algorithms involved in processing data, and the context in which the technology is deployed. As such, the reliability of different biometric technologies may differ, sometimes significantly. Such subtleties tend not to inform the more basic use of biometrics which seems to the public to be reliable or at least unproblematic much of the time. In simple terms, the fact that a smartphone seems to work reliably by use of a thumbprint tells one little about the reliability of related technologies deployed in the criminal justice field to identify or exclude possible suspects.

Public Awareness

3.8 Increased use of biometrics appears to be technology driven, i.e. simply because the technology is available. Consideration of the risks that these technologies present[50] and their human rights implications have not received the public attention they deserve, despite the efforts of some politicians and journalists, and the UK Biometrics Commissioner in his annual reports and other statements. Of course, the UK Commissioner's role in Scotland is confined to reserved matters which means he receives less publicity here than in England. In addition, the limitations of the technologies are not well understood. All biometrics technologies are subject to measurement uncertainty and their accuracy (false positives, i.e. mistaken identifications, and false negatives, i.e. mistaken exclusions) are rarely fully understood. This can affect public confidence in such technologies.

3.9 Some biometric data are captured with consent, for example, DNA (the Guthrie new-born test), airport security images. However, much biometric data can now be captured without consent or the awareness of the individual concerned, for example, images obtained from public space CCTV.

3.10 More specialist use of biometric technologies is also developing. One recent example is facial recognition technology which has attracted publicity in terms of both effectiveness and unreliability, with evidence and arguments supporting each opposing view.

3.11 There needs to be a wider debate about the various implications of the capture or surrender of biometric data, especially in terms of the implications for privacy. Privacy is not an infinite commodity. Bit by bit, especially in the capture or surrender of biometric data, a detailed profile of individuals can be assembled. The current reality is of increasing capture of biometric data by public bodies and private companies. Whether, and, if so, how, such data can also be accessed by the police is another area deserving of publicity, discussion and debate.

3.12 There are two different public discussions that we wish to see: first, discussion and debate of the specific proposals in this report, and, second, discussion and debate of

---

[50] See, for example, the following Guardian story from 4 January 2018 – https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar: 'The personal information of more than a billion Indians stored in the world's largest biometric database can be bought online for less than £6, according to an investigation by an Indian newspaper.
The reported breach is the latest in a series of alleged leaks from the Aadhaar database, which has been collecting the photographs, thumbprints, retina scans and other identifying details of every Indian citizen.
The report … claimed that software is also being sold online that can generate fake Aadhaar cards, an identity document that is required to access a growing number of government services including free meals and subsidised grain.'

broader issues such as whether regulation should extend beyond policing or beyond the public sector. It is important that both areas start to form part of the discourse which starts before public consultation.

3.13 It is important to improve levels of awareness, including awareness of any relevant minimum retention periods and opportunities to apply for deletion. While this does happen at present, it is not something which is publicised or widely known. No special steps are taken to assist the understanding of those with vulnerabilities which might affect the question of consent, and the extent to which it is fully informed.

3.14 We need clarity of purpose for all use of biometric data, with discussion about the extent to which the public is prepared to accept data linkage. There is likely to be increased movement towards convergence of different databases, for example, certain information on UK border control databases being linked to broader criminal justice databases. Sometimes such linkage may bring improvements and advantages, but it may also bring increased risks. Such data linkage should be subject to regulation and oversight and adhere to human rights and ethical principles.

3.15 Debate and discussion should address gaps in knowledge and understanding. This will assist in preparation for emerging technologies as the public, as well as police and others, become increasingly dependent on biometrics in their daily personal and working lives.

3.16 The extent of public knowledge and concern, or otherwise, should be gauged to inform possible public awareness campaigns. Consideration should be given to including suitable questions in the Scottish Social Attitudes Survey. While answers from the fuller survey could not be provided in time to inform the public consultation to follow our recommendations, it may be possible, in the shorter term, to use Scot/Cen's smaller panel survey[51]. This could gauge public awareness, knowledge and confidence in relation to existing and developing biometric technologies, especially with regard to privacy and other ethical and human rights aspects. Information from these surveys can inform the development of policies and rules in the future, as well as offering some guidance to the Commissioner about areas of concern.

3.17 There are courses available in schools to teach online safety. It may be appropriate to expand these to include greater information about awareness of sharing personal data, including biometric data.

---

[51] http://www.natcen.ac.uk/our-expertise/methods-expertise/surveys/probability-panel/ http://www.natcen.ac.uk/our-expertise/methods-expertise/surveys/probability-panel/.

3.18 We envisage increased media engagement by biometrics experts (e.g. Professor Sue Black, Professor Jim Fraser). 2017 saw an increased public interface between crime writers and the legal profession, with discussions about the authenticity of crime fiction leading some writers to engage also with experts in forensic science. Other opportunities are being explored, as film-makers and TV companies seek to use authentic technology and real-life knowledge in presenting their stories[52].

3.19 We see the website of the Commissioner as a valuable resource for disseminating information about biometric technologies and the use of biometric data. The Commissioner can arrange for work to be done to evaluate the effectiveness of biometric databases, something not done so far. The Commissioner can also work with public and other bodies in the field to seek to establish better reporting of their procedures and outcomes for the purposes of offering reassurance to the public and thereby providing confidence at an appropriate and justified level, managing expectations against greater awareness of the limits of reliability.

3.20 From our work, it is apparent that a number of individuals and organisations, academic and other, take an interest in developments in this area, including the ethical aspects of such developments. Many of them contributed written and other submissions to our Group. The Commissioner should be able to use some of that experience and expertise in seeking to increase awareness.

3.21 Lessons can be learned from similar work in England and Wales. In particular, it seems to assist public awareness when fairly specific and detailed case studies are provided on such websites.

3.22 The issues are of sufficient importance to require well-informed discussion and debate at the Scottish Parliament, both in the Chamber and by consideration at various committees whose work touches on the subject-matter, for example, Justice, Equalities and Human Rights, Health and Sport, Education and Skills. We have already engaged with members of the Scottish Youth Parliament who have agreed to discuss how best to engage with the subject there, with the likelihood of a full debate in the Youth Parliament at some point in 2018.

3.23 There is a role too for Government. Useful lessons might be learned from the experience of the UK Government in its response to the various Public Attitudes to Science surveys.

---

[52] http://www.heraldscotland.com/news/15784999.Forensic_officers_in_Scotland_to_market_their_expertise_to_TV_crime_shows/ http://www.heraldscotland.com/news/15784999.Forensic_officers_in_Scotland_to_market_their_expertise_to_TV_crime_shows/.

3.24 While our recommendation in this area may be more aspirational than in other Chapters, we consider the issue of public awareness to be of sufficient importance to be highlighted in this way.

Recommendation 1

There should be national debate to improve public understanding of, and confidence in, the retention and use of biometric data in Scotland for policing, law enforcement and other public protection purposes. Ideally, this should start before and continue during the Scottish Government's public consultation, as well as featuring in ongoing discussion after consultation.

4 The Law – Human Rights and Data Protection

This Chapter is in two parts – Human Rights and Data Protection.

4.1 For the current legal position in Scotland, see Chapter 2 above. It is also worth considering the attitude of the courts in Scotland to 'new' sciences, especially as some developing biometrics have not yet been accepted or tested in our courts. While normally the Court will intervene only upon challenge by the defence or Crown to the admissibility of such evidence, it seems likely that, with increasing emphasis on effective case management by the judiciary, the Courts may become more pro-active. In any event, the Courts in Scotland are alive to issues relating to the testing of reliability and admissibility of new technologies[53].

4.2 Human rights are a key consideration in this area, deserving of detailed attention. The European Court of Human Rights has considered challenges to the capture and retention of biometric data, as well as other related matters. Further challenges are in the pipeline[54]. It seems likely that there may be developments in jurisprudence about the proportionality of indefinite retention of biometric data without any supporting evidence or gravity threshold for the triggering conviction, an area commented on without approval in *S* and *Marper v the UK* in which the Court pointed out:

> 'The United Kingdom thus also appears to be the only member State expressly to allow the systematic and indefinite retention of both profiles and samples of convicted persons. Complaint mechanisms before data-protection monitoring bodies and/or before courts are available in most of the member States with regard to decisions to take cellular samples or retain samples or DNA profiles.'[55]

4.3 As discussed below in Chapter 8, any such development would necessitate reconsideration of current Scottish legislative provision for the retention of DNA and fingerprints.

4.4 With thanks to our Advisory Group colleague, Diego Quiroz, this Chapter starts in Part 1 with extracts from a paper he prepared to assist in a detailed human rights appreciation of this area. Diego's full paper will be published along with the report.

---

[53] International Society for the Reform of Criminal Law Conference Crossing Boundaries: Exploitation, e-Crime, Evidence, and Extradition21 - 25 June 2015 - Edinburgh, Scotland - Papers by Lord Turnbull (Expert Evidence and the Changing Role of the Trial Judge) and the Right Honourable Lord Bracadale (Expert Evidence: The Admissibility as Expert Evidence of Case Linkage Analysis in Thomas Ross Young v HMA).

[54] *Gaughran v UK* (Application number 45245/15) and *Catt v UK* (Application number 43514/15)).

[55] Paragraphs 48 and 49.

4.5 Data protection is another key area when it comes to biometric data. We are grateful to Ken Macdonald, Head of ICO Regions for providing the helpful summary which completes the Chapter in Part 2.

Part 1

Human rights – introduction

4.6 The purpose of this section is to provide a short overview of the human rights framework around the use of biometric data for law enforcement purposes in Scotland, and the associated biometric data retention regime (in relation to the retention and disposal of DNA, fingerprints and photographic images).

4.7 The first part of this section is an overview of the key human rights considerations that should be taken into account in relation to the use of biometric data, including use by private actors when performing public functions. The second part examines how a human rights based approach could be applied when thinking about a framework for the use of biometrics.

4.8 There are strict human rights obligations, derived from the Human Rights Act 1998 ('HRA'), and human rights standards emerging from international human rights treaties, that would help public authorities to ensure any new framework is fit for purpose. The Equality Act 2010 sets a number of general and specific duties for public sector organisations[56] in relation to non-discrimination[57]. As a starting point, and as recommended by the Council of Europe, the introduction and use of new technologies should take full account of, and not contravene, fundamental principles such as the inherent dignity of the individual and respect for the human body, the rights of the defence and the principle of proportionality in the provision of criminal justice[58].

4.9 From the outset, it is important to note that there is a lack of evidence on the effectiveness/reliability of some biometric technologies (e.g. facial images)[59] currently used by law enforcement agencies[60]. There is a need for an effective assessment of the benefit of these technologies to ensure that any new regime is based on utility and public safety and derives from sound evidence rather than

---

[56] A private (or a voluntary) body is subject to the general duty in respect of any public functions which it has.
[57] The list of bodies which are subject to the general duty found in Schedule 19 of the Act and includes key public authorities like local authorities, the police, the armed forces and central government departments.
[58] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
[59] Facial images are just the first of a new wave of biometrics.
[60] Biometrics Commissioner, annual report 2017, para 36 and Biometrics – Independent Advisory Group Review, Scotland. Big Brother Watch submission, 12th September 2017.

anecdote or impression[61]. It is also crucial to ensure that there is greater transparency and public participation around the use of biometric data in the criminal context[62].

4.10 Nowadays, a significant shift has been made, as biometrics is used more and more in the private sector, primarily due to technological developments and investment by the private sector. There is a legitimate expectation that private actors (e.g. business enterprises dealing with the use of biometric data in different ways) should comply with all applicable laws and respect human rights[63]. Furthermore, the Government has a duty to take appropriate steps to prevent, investigate, punish and provide redress for human rights abuses committed by private actors.

Human Rights Law

4.11 The HRA, which incorporates the European Convention on Human Rights (ECHR) into UK law, sets out the fundamental rights and freedoms that everyone in the UK is entitled to, and makes it unlawful for a public authority to act in a way which is incompatible with Convention rights.

4.12 It is paramount that the relevant public authorities put in place an effective human rights framework when biometrics are used by law enforcement agencies. This framework should also reflect ethical considerations, and the values of the people living in Scotland.

4.13 Other international standards in relation to the storage and management of data include the Council of Europe Convention 108[64], European Union (EU) instruments such as Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data[65], as well as the case law of the Court of Justice of the European Union and the EU Charter on Fundamental Rights[66].

4.14 As a consequence, any policy and legal framework for its use must be consistent with the human rights framework, and other guarantees laid down by relevant data protection laws. The use of personal data is sensitive and must be protected from

---

[61] Biometrics Commissioner, annual report 2017, para 36 and Biometrics – Independent Advisory Group Review, Scotland. Big Brother Watch submission, 12th September 2017.
[62] The difficult judgment as to the proper balance between public and private interest in a democratic society is best taken by Parliament in the first instance, expressed through legislation. It should not be left to the agencies using the data.
[63] See UN Guiding Principle on Business and Human Rights. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
[64] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[65] See, for example, Directive 2016/680 as well as Regulation (GDPR) 2016/679. Both refer in detail to biometric data. The EU Charter on fundamental rights is also quite specific on rules of rights to privacy.
[66] e.g., Arts. 7 and 8.

abuse and arbitrariness. In this light, complaint and regulation mechanisms are important and necessary safeguards against arbitrariness.

Article 2 – the Obligation of the State to Protect the Right to Life

4.15 Article 2 safeguards the right to life and sets out the circumstances when deprivation of life may be justified. This is one of the most fundamental provisions in the Convention which imposes a duty to protect life through taking practical steps to address situations where there is an identifiable and real threat to life, including from attacks by other private individuals. The action required must be reasonable without imposing an impossible or disproportionate burden on the authorities.

4.16 This Article is relevant to the investigation by the State of murder and other serious crime.

Article 8 – the right to respect for private life, home and correspondence

4.17 It is acknowledged that the acquisition and retention of biometric data plays a role in criminal justice policy and practice. However, such practices can engage the reasonable expectation of privacy that people have[67]. It is therefore crucial that there are safeguards in place to ensure the right of the public to be protected from crime is balanced with the rights of the individual.

4.18 Article 8 of the ECHR and the HRA require respect for private and family life, home and correspondence. These concepts are sometimes indistinguishable and cover the protection of the moral and physical integrity of the individual. Article 8 therefore encompasses a wide range of issues. Biometric data can contain a significant amount of sensitive information about an individual's identity, including information about their health[68] and their unique genetic code.

4.19 In *S and Marper v the UK*, the European Court of Human Rights (ECtHR) stated that:

> 'the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests… The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.'"[69]

---

[67] Ibid.
[68] It is argued that facial recognition technology is becoming increasingly able to predict personal information, such as health conditions. See National DNA Database Ethics Group, Notes of the 38th meeting held on 7 June 2017 at Home Office, 2, Marsham Street, Westminster, London, SW1P 4DF.
[69] *S and Marper v the UK* (Applications nos. 30562/04 and 30566/04) at paragraph 112.

4.20 The Court referred to a Canadian Supreme Court case (*R v RC*[70]) which considered the issue of retaining a juvenile first-time offender's DNA sample on the national database. The court upheld the decision by a trial judge who had found, in the light of the principles and objects of youth criminal justice legislation, that the impact of the DNA retention would be grossly disproportionate. In his opinion in that case, Fish J observed:

> 'Of more concern, however, is the impact of an order on an individual's informational privacy interests. In R v Plant, the Court found that section 8 of the Charter protected the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state". An individual's DNA contains the "highest level of personal and private information": S.A.B. Unlike a fingerprint, it is capable of revealing the most intimate details of a person's biological make-up. ... The taking and retention of a DNA sample is not a trivial matter and, absent a compelling public interest, would inherently constitute a grave intrusion on the subject's right to personal and informational privacy.'

4.21 Article 8 of the ECHR is a qualified right, which requires the State to justify any interference by reference to its legality and necessity. So, any restrictions should be:

- In accordance with the law: 'requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct'[71];
- In pursuit of a legitimate aim: a public authority which intends to interfere with a person's rights under Article 8 must be able to demonstrate that such interference is based on one of the legitimate aims set out in Article 8(2), including '*the prevention of disorder or crime'* and 'the *protection of the rights and freedoms of others*'[72]; and
- Necessary in a democratic society: 'An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient'[73]. In terms of assessing proportionality, three main issues are relevant:

  a) the degree of the interference;

[70] [2005] 3 SCR 99, 2005 SCC 61.
[71] Ibid.
[72] See *Khan v the UK* Application No 35394/97 (ECHR)
[73] As above in footnote No. 8.

b) whether there were less intrusive means available; and

c) the procedural safeguards available.

4.22 An alternative formulation of proportionality was given by Lord Reed in a UK Supreme Court case (*Bank Mellat v Her Majesty's Treasury*[74]):

> [I]t is necessary to determine (1) whether the objective of the measure is sufficiently important to justify the limitation of a protected right, (2) whether the measure is rationally connected to the objective, (3) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and (4) whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter.

4.23 The use, including both the collection and retention of biometric data, is by its nature intrusive. There is a need for greater clarity about when the police or law enforcement agencies may collect biometric data from a person without their consent.

4.24 While matters are relatively clear in relation to fingerprints, that is not the case for other biometric data. The use of facial biometrics and facial biometric recognition systems, which are used for intelligence/investigative purposes, is far more intrusive than CCTV, and can be taken without knowledge or consent. Public interest and public safety are paramount, however a rights-based legal framework that respects Article 8 should be in place to guard against the risks of misuse[75].

4.25 Examples of physiological characteristics used for biometric authentication include fingerprints and DNA. The use of databases and DNA retention has come into question in the United Kingdom. This includes *R (RMC and FJ) v MPS (Metropolitan Police Service)*[76] where the court held that the retention of custody photographs amounted to an unlawful interference with R's and F's Article 8 rights. In *S and Marper v the UK*, the European Court of Human Rights (ECtHR) was '*struck by the blanket and indiscriminate nature of the power of retention in England and Wales*' of DNA and the '*fact that the same rules applied to juveniles (such as S) as to adults, despite the need to consider children differently under the criminal justice system to comply with the UN Convention on the Rights of the Child*'.[77] The Court commented

---

[74] [2013] UKSC 38

[75] In *Klass v. Germany* (Application no. 5029/71) for example, the European Court of Human Rights stated that it must be satisfied that any system of secret surveillance conducted by the State must be accompanied by adequate and effective guarantees against abuse.

[76] [2012] EWHC 1681 (Admin).

[77] Article 40 of the CRC, for example, sets out children's rights in the criminal legal system.

also on '*[T]he need for such safeguards …[being] all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.'*

4.26 In relation to the margin of appreciation, the ECtHR articulated in *S and Marper v the UK*:

> 'A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted.[78] Where, however, there is no consensus within the Member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider.'[79]

4.27 A key consideration is the length of time for which data are stored. Useful guidance can be found in *S and Marper* and the Committee of Ministers' Recommendation No. R (92)1 and R 87 (15)[80] which advises that personal data kept for police purposes should be deleted if it is no longer necessary for the purposes for which it was stored. So, biometric data taken from individuals should be routinely deleted when it is no longer necessary to keep them for the purposes for which they were collected. A blanket policy on retention of any type of biometric data of persons suspected, but not convicted, of offences does not strike a fair balance between private and public interests. In light of this test, it is difficult to see how there can be sufficient justification to retain biometric data indefinitely.

4.28 Both international and national courts have found that the blanket retention of biometric data (DNA profiles, cellular samples and fingerprints and custody photographs) is unlawful and constitutes an unjustified interference with the right to respect for private life, in violation of Article 8 of the ECHR[81]. The UK response to the *Marper* case was, in part, the Protection of Freedoms Act 2012 (PoFA), which introduced regulation and restrictions where their absence had been criticised. The 2012 Act also established the office of the UK Biometrics Commissioner.

---

[78] See *Evans v. the United Kingdom* Application No. 6339/05 (ECHR)).
[79] see *Dickson v. the United Kingdom* Application No. 44362/04, (ECHR)).
[80] Recommendation No. R 87 (15) to member states regulating the use of personal data in the police sector.
[81] R (RMC and FJ) v MPS (Metropolitan Police Service) [2012] and R (on the applications of S and Marper) v Chief Constable of South Yorkshire' [2004] 1 WLR 2196, [2004] 4 All ER 193.

4.29 It is worth noting that in *S and Marper,* the ECtHR praised Scotland for the choice of time limits on retention of DNA. The ECtHR also suggested that the indefinite retention of the DNA of even convicted persons was not acceptable as a blanket policy, although the legal landscape relating to retention post-conviction is less clear and probably not finally settled. In the UK Supreme Court case of *Gaughran v Chief Constable of the Police Service of Northern Ireland*[82], the majority held that the blanket policy of retaining DNA profiles from all convicted persons was within the margin of appreciation, and proportionate and justifiable interference under Article 8(2). There was a strong dissent by Lord Kerr who argued that the policy was not rationally connected to the objective of countering crime as there is no evidence that indefinite retention of biometric data of all persons convicted of a recordable offence in any way contributes to the detection and identification of future crime. He further argued that the policy failed to strike a fair balance between the rights of society and those of the individual, concluding that 'clearly, a far more nuanced, more sensibly targeted policy can be devised'[83]. The case is awaiting consideration at the ECtHR.

4.30 There are questions in relation to what 'convicted' means e.g. cautions, reprimands and final warnings, and the proportionality of retaining data indefinitely in such cases. *Marper* requires the UK Government to give detailed consideration to the use or planned use of other biometric technologies (including facial images) which must meet Convention requirements.

4.31 One of the key points under human rights law is that biometric data constitute personal data. As a consequence, any policy and legal framework for its use[84] must be consistent with the human rights framework, and other guarantees laid down by relevant data protection laws.[85] The use of personal data is sensitive and must be protected from abuse and arbitrariness.[86]

Impact on other human rights

4.32 The use of biometric data by law enforcement agencies engages a number of human rights beyond Articles 2 and 8 of the ECHR. Law enforcement agencies should give due consideration to the use of biometrics and its impact on other human rights and fundamental freedoms. These include:

- The prohibition of torture, inhuman, degrading treatment or punishment (Article 3 of the ECHR)
- The right to liberty and security (Article 5 of the EHCR)

---

[82] [2015] UKSC 29.
[83] Ibid at para 83.
[84] Use includes collection, capturing, retention and deletion of records for those who are found innocent or are not convicted of a criminal offence.
[85] See Data Protection Act 1998.
[86] Hammarberg, T (2008) 'More Control is Needed of Police Databases. Human Rights in Europe, Viewpoints by the Commissioner for Human Rights'.

- Due process and the right to a fair trial (Article 6 of the ECHR)
- Freedom of religion (Article 9 of the ECHR)
- Freedom of expression and association (Article 10 and 11 of the ECHR)
- The principle of non-discrimination (Article 14 of the ECHR)

4.33 More detailed reference to the potential relevance of Articles 3, 5 and 6 is given in the full text of the Human Rights paper by Diego Quiroz.

4.34 Effective law enforcement and the protection of human rights are complementary and mutually reinforcing objectives, which must be pursued together as part of States' duty to protect individuals' rights and freedoms within their jurisdiction.

Articles 9 to 11 – democratic freedoms

4.35 Human rights are legal guarantees which protect individuals and groups against actions and omissions that interfere with fundamental freedoms and human dignity. Democratic freedoms are fundamental to the existence of a democratic society, where views, ideas and information can be exchanged. These freedoms include the right to respect for freedom of expression, assembly and association, and freedom of thought, conscience and religion.

4.36 While there is a general requirement to refrain from unjustified interference, there may be situations where law enforcement agencies are justified in doing so. However, any interference with these rights must comply with a number of conditions if it is to be consistent with the Convention.

4.37 The use of biometric data without the consent of the individual and, in particular, while exercising their fundamental freedoms of religion, assembly or association would not only be a significant interference with Article 8 but will engage these other rights. It is worth noting that indiscriminate practices may have a severe, unintended and inhibiting effect on the exercise of our democratic freedoms. Therefore, the authorities should ensure that any relevant operation, for example, the policing of public protests and demonstrations, complies with human rights norms and international standards. On this point, see also paragraph 2.6 of the submission to the IAG by No2ID Scotland.

Equality and non-discrimination

4.38 The principles of equality and non-discrimination are central to human rights law and are recognised as norms in both the domestic and international framework[87]. In line with this, the Government should ensure that the principle of non-discrimination is

[87] Case concerning the Barcelona Traction, Light and Power Company, Limited, Second Phase, Judgment of 5 February 1970, ICJ Reports (1970), p. 3, at p. 32. – in relation to racial discrimination.

interpreted and applied consistently by law enforcement agencies. The practice of collecting, retaining and deleting biometric data should afford special consideration to the situation of vulnerable and disadvantaged groups, including children.

4.39 While the use of biometric data to profile potential suspects may, in principle, be a permissible means of investigation and can be an important law enforcement tool, it is important that enforcement agencies do not use broad profiles that reflect unexamined generalisations and/or stigmatisation. The European Union Network of Independent Experts on Fundamental Rights has expressed serious concerns about profiling[88] on the basis of characteristics such as nationality, age or birthplace. These experts have recommended that profiling must strictly comply with the principles of necessity, proportionality and non-discrimination as well as being subject to close judicial scrutiny and periodic review[89].

4.40 There is a risk that certain groups are disproportionately affected by collection and retention measures in this area. The UK DNA database holds about a third of all black men and about three quarters of all young black men (aged 16 to 34) resident in the UK, and the proportion of the Asian population held on the DNA database is steadily increasing. People with mental illness are also over-represented on the database[90]. The collection and retention of biometric data of these groups may compound and increase other institutional or societal discrimination or bias.

4.41 According to established jurisprudence of the ECtHR and international human rights bodies, any measures having the purpose or effect of creating a difference in treatment (based on a prohibited ground), which are not reasonably or objectively justified, are discriminatory[91].

A Human Rights Approach to Biometrics

4.42 Human rights should continue to be mainstreamed into the strategies, policies and operational processes of policing[92]. The IAG advocates a human rights based approach to the use of biometric data. The key principles of this approach are: legality, accountability, effective participation, non-discrimination and empowerment. For further detail, see the full text of the Human Rights paper by Diego Quiroz.

---

[88] Profiling is a filtering process involving a single indicator or a cluster of indicators that, when grouped together, present the characteristics of a high-risk person, passenger or consignment.
[89] E/CN.4/2005/103, paras. 71–76.
[90] The Equality and Human Rights Commission's response to the government's consultation on: Keeping the right people on the DNA database (2009) p 5.
[91] See Abdulaziz, Cabales and Balkandali v. the United Kingdom (ECHR).
[92] See for example human rights based policing at http://www.scottishhumanrights.com/justice/policing/#policing-1244.

4.43 The human rights framework for biometric data should also have an effective, accessible and independent mechanism of review for the individuals concerned. For example, there should be provision for independent review of the justification for the retention of biometric data according to defined criteria, including such factors as the seriousness of the offence, previous arrests, utility of the retention and period of retention, the strength of the suspicion against the person and any other special circumstances. Individuals should be provided with an effective remedy to challenge the storage of biometric data and its use[93]. A formal scheme for destruction ensures accountability and community trust in the system. Complaint mechanisms play an important role in protecting against potential abuses and arbitrariness.

4.44 Sufficient information regarding the governance and management of biometric data should be in the public domain to maintain transparency, accountability and public confidence in their use[94].

ECHR – Other relevant cases

4.45 It is worth noting two other relevant ECtHR cases. First, *Peruzzo and Martens v Germany*[95] in which the applicants, who had been convicted of serious criminal offences, complained about the domestic court's orders to collect cellular material from them and to store it in a database in the form of DNA profiles for the purpose of facilitating the investigation of possible future crimes.

4.46 The Court declared the application inadmissible as manifestly ill-founded. It found that the domestic rules on the taking and retention of DNA material from persons convicted of offences reaching a certain level of gravity as applied in the case of the applicants had struck a fair balance between the competing public and private interests and fell within the respondent State's acceptable margin of appreciation.

4.47 And, second, *Affaire Aycaguer v France*[96] in which the applicant alleged that there had been a breach of his right to respect for his private life on account of the order to provide a biological sample for inclusion in the national computerised DNA database (FNAEG) and the fact that his refusal to comply with that order had resulted in a criminal conviction.

4.48 The Court held that there had been a violation of Article 8. It observed in particular that in 2010 the Constitutional Council had declared the provisions on the FNAEG to be in conformity with the Constitution, subject, *inter alia*, to 'determining the duration of storage of such personal data depending on the purpose of the file stored and the

[93] *Segerstedt-Wiberg and Others v. Sweden*, application no. 62332/00 (ECHR)
[94] *S and Marper v UK*, para 99 (ECtHR)
[95] 7841/08 and 57900/12, 4 June 2013 (admissibility decision)
[96] Requête no 8806/12 22 June 2017

nature and/or seriousness of the offences in question'. The Court noted that, to date, no appropriate action had been taken on that reservation and that there was currently no provision for differentiating the period of storage depending on the nature and gravity of the offences committed. The Court also ruled that the regulations on the storage of DNA profiles in the FNAEG did not provide the data subjects with sufficient protection, owing to its duration and the fact that the data could not be deleted. The regulations therefore failed to strike a fair balance between the competing public and private interests.

ECHR – Outstanding cases

4.49 Two relevant cases are awaiting consideration by the ECtHR, in addition to *Gaughran*. One is *Catt v ACPO*[97] in which the UK Supreme Court held that the retention of personal data, including photographs, of a person who is not suspected of any criminality for an undefined period of time was acceptable[98]. In another strong dissent, Lord Toulson argued that the policy was not proportionate as the police had not justified the value of retaining the information on Catt. He also noted that the police had not argued that removing it would be impractical – this had been presumed by the court.

4.50 In *JJ and SU v UK*[99], the ECtHR will consider the Safeguarding Vulnerable Groups Act 2006 (English legislation) which introduced 'barred lists' that, in effect, precluded the individual from working with the relevant group, whether adult or child. The applicants were included in the barred lists after being convicted of, and cautioned for, a criminal offence respectively. They were not given an opportunity to make representations before inclusion in the lists. However, various options were open to them to challenge their inclusion. Again, issues of necessity and proportionality will be considered which may also be relevant to the retention of biometric data.

4.51 For additional human rights consideration of the issues, see also the Justice Scotland submission to the IAG.

[97] Application number 43514/15.
[98] [2015] UKSC 9.
[99] Application numbers 31127/11 and 8114/13.

Part 2

Data Protection and Biometrics – introduction

4.53 Data Protection legislation in the UK and throughout the wider EU provides a framework for the handling of personal data. In summary, personal data are data which relate to a living individual who can be identified from it directly or with other information which is in the possession of, or is likely to come into the possession of, the data controller (i.e. the organisation using the information).

4.54 The current Data Protection Act 1998 (DPA) transposes into UK law the provisions of the European Data Protection Directive 95/46/EC. Along with associated Regulations, the DPA provides the legal framework for all processing of personal data throughout the UK. However, in May 2018, a new data protection regime will apply throughout the EU as a consequence of adoption by the EU of the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). The LED will be transposed into UK law through the Data Protection Bill 2017 (DPB) which is currently being considered by the Westminster Parliament. The Bill will also legislate on matters contained within the GDPR which have been derogated to individual Member States.

The Revised Data Protection Regime

4.55 As indicated above, the European data protection regime will change with effect from May 2018. General processing of personal data must be undertaken in compliance with the GDPR and processing for law enforcement purposes by designated or 'competent' authorities – i.e. named authorities with powers to investigate and/or prosecute crimes and impose sentences, together with certain other organisations -– must conform with the LED however transposed into domestic law. The GDPR contains a number of derogations to Member States and these, as well as the transposition of the LED into UK law, are being considered within the DPB. The new Data Protection Act is expected to be passed in February 2018.

4.56 The GDPR extends the current data protection regime in a number of ways. It updates the definition of personal data to reflect scientific and technological advances which have taken place since the passing of Directive 95/46/EC; it provides a number of enhanced rights for data subjects; and it requires data controllers to strengthen their governance procedures in relation to personal data. Similar changes are seen in within the law enforcement provisions of the DPB.

4.57 As with the existing regime, the GDPR is framed around a number of principles. Although worded slightly differently, the new set reflect the current ones. They require that personal data are:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.58 Both GDPR and the law enforcement provisions require that the controller shall be responsible for, *and be able to demonstrate*, compliance with the principles. This includes a presumption of privacy by design, i.e. building protection into data handling policies and procedures. Additionally, the law enforcement provisions of the DPB require that logs are kept of any automated processing of personal data, i.e. where a system undertakes processing by automated means. The logs required include collection, alteration, consultation with, disclosure, combination and erasure of personal data records.

4.59 Both the GDPR and the law enforcement provisions adopt a definition of personal data which explicitly includes biometric information within it as a 'special category'. Any processing of biometric information must therefore be undertaken in compliance with either the GDPR or the new Data Protection Act (when enacted) according to whether the processing is general processing or for law enforcement purposes. In this regard, biometric data are defined as '*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic* [i.e. fingerprint] *data*'[100].

4.60 The processing of biometric data is only permitted in the GDPR where one of a number of conditions apply. These include consent, for the vital interests of the data subject where the subject is incapable of giving consent, for the establishment, exercise or defence of legal claims or if courts are acting in their judicial capacity and for reasons of public interest in the area of public health. However, the derogations granted to Member States allow extensions and/or exemptions to these conditions to apply under certain circumstances. The DPB therefore proposes additional conditions for processing such as for preventing and detecting unlawful acts.

[100] GDPR Article 4, paragraph 14 - http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

4.61 Moreover, where a controller is a competent authority as defined in schedule 7 of the DPB and is processing for law enforcement purposes (the prevention, investigation, detection or prosecution of criminal offences), there are further restrictions on the conditions for processing which can be used. Although outwith the remit of this Group, it should be noted that there are also restrictions on the conditions for processing which can be claimed by the intelligence services.

4.62 Both the GDPR and the law enforcement provisions require that where processing is likely to result in a high risk to the rights and freedoms of individuals, a data protection impact assessment (DPIA, previously known as a Privacy Impact Assessment or PIA) should be undertaken. The assessment must consider the risks to the rights and freedoms of the data subjects, the measures envisaged to address these risks and the safeguards, security measures and mechanisms to ensure the protection of the data. Where the processing is likely to result in a high risk to the rights and freedoms of the individuals (in the absence of mitigations), the data controller must consult with the Information Commissioner.

Regulation

4.63 Regulation of the new data protection regime will be the responsibility of the UK Information Commissioner. Individuals may raise concerns about the manner in which their personal data have been handled, and compliance with their rights contained in the GDPR and the law enforcement provisions, with her. In this regard she will have enhanced powers of assessment and enforcement and she will be statutorily required to issue guidance on how she proposes to exercise her functions relating to assessment notices, enforcement notices and penalty notices. Failure to comply with a notice served by the Commissioner will continue to be a criminal offence. In addition, data controllers will be required to notify the Commissioner of any security breach which is likely to result in a risk to the rights and freedoms of individuals within 72 hours of it having been discovered (and, where there is a high risk to those rights and freedoms, the affected individuals must be notified too).

4.64 The Commissioner's ability to serve civil monetary penalties following the breach of any of the data protection principles will be much enhanced following implementation of the new regime. In the most severe cases, where individual rights are at greater risk of being compromised, the maximum penalty will be the greater of 4% of annual turnover or €20m, whilst, for other breaches, the maximum penalty will be the greater of 2% of annual turnover or €10m. In addition, failure to report a notifiable security breach within the statutory time period may result in a further penalty of the greater of 2% of annual turnover or €10m being imposed.

5 General Principles and Ethical Considerations

5.1 This Chapter overlaps with Chapter 4, with the various human rights and data protection principles often similar and equally relevant in addressing ethical considerations. It is important to ensure a proper grasp of ethical considerations at all stages of the biometrics data process – acquisition, use, retention and disposal – given the highly sensitive and personal nature of the data involved. It is important to ensure that what is done is informed by considerations of what should be done, as opposed to merely considerations of what can be done. Or, as it was put in the medConfidential submission to the IAG, '*Just because something can be done somewhere, does not mean it should always be done everywhere.*'

5.2 Much work has been done by others to identify relevant human rights and other ethical principles relevant to biometric data. We have not needed to innovate, instead pulling together some of these from elsewhere, borrowing especially from a helpful paper produced by the Biometrics and Forensics Ethics Group ('*BFEG*'), the body that provides advice to Home Office in this area. We are grateful to them for sharing this paper which had not yet been published. We have, however, adapted it with regard to our work and the Scottish context, insofar as involving any different considerations. Appendix 4 includes related questions from the same BFEG paper which assist in focussing the principles.

5.3 We consider that these principles might usefully feature in the Code of Practice and could therefore form part of the public consultation. They should apply to all public bodies operating in this area. Private bodies should also apply them. Public bodies dealing with private bodies should ensure that their partners in the private sector operate in accordance with these principles.

5.4 The principles take into account the particular context of the relevant science, with validation a key and distinct concept to offer assurance around reliability, efficiency and effectiveness.

5.5 Acceptance of these principles should not stifle progress but may help to ensure that there is always sufficient pause for thought and review before proceeding. As this area relates to existing, emerging and future technologies, it is important that issues of quality are addressed in each. Validation is one key means of addressing issues about the quality of the underlying biometric technologies.

General principles

5.6 The use of biometric technologies and forensic procedures should comply with the following governing principles:

- enhance public safety and the public good;
- advance the interests of justice;
- respect for human rights of individuals and groups;
- respect the dignity of all individuals;
- take particular account of the rights of children;

- take particular account of the rights of other vulnerable groups and individuals;
- protect the right to respect for private and family life;
- scientific and technological developments should be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims, and assist the criminal justice process;
- based on validated evidence. (See below regarding validation).

Implementation of the General Principles

5.7 The general principles should be implemented with due regard to the following:

- impartiality – procedures should be applied without bias or unfair discrimination;
- proportionality – balancing individual rights, public safety and the public good;
- effectiveness;
- openness and transparency;
- minimal intrusion needed to achieve outcome;
- the need for systems to be validated to show that they are fit for the specific purpose intended i.e. the results can be relied on irrespective of use (for example, intelligence or evidential purposes);
- the need for assurance in relation to the quality of the system;
- the need for public accountability;
- the need for independent oversight where appropriate;
- the need to provide adequate information and, where appropriate, to obtain consent from those from whom data or samples are sought or retained, or from some other appropriate individual where the individual cannot consent

Considerations Specific to the Collection and Processing of Data

5.8 In relation specifically to the collection and processing of data the governing principles should be applied as follows:

- data should be collected, stored, used and retained only for specified and lawful purposes;
- data collection, storage, and use must adhere to legal requirements;
- steps should be taken to ensure the accuracy, security and integrity of data collected, stored and used;
- steps should be taken to ensure transparency around error rates and uncertainties inherent in the procedures;
- processes should be robust and conform to any relevant standards and be applied by professionally trained staff whose work can be audited;
- intrusion into private lives should be minimised – this may be of particular significance in relation to issues of data linkage;
- account should be taken of the interests of secondary data subjects (i.e. people potentially affected by data collected from others, e.g. family members);

- policies should be in place around the weeding and disposal of these data, including a presumption in favour of deletion.

Validation

5.9 To comply with the governing principles set out above it is important that the effectiveness and reliability of any biometric technologies is established by those who use them. The key issue is that all technologies should be fit for purpose i.e. capable of achieving the outcome that they are designed to achieve. Further considerations are the efficiency and cost effectiveness of any technologies. An important consideration is that the user should not simply rely uncritically on third party assertion regarding the performance of technology without an understanding of how the technology performs **as it is applied by the particular user and for the particular purpose of that user**. Biometric technologies that are perfectly adequate for individual users to protect their data or privacy may not be adequate for use at the level of an organisation or in a criminal justice context.

5.10 One means of establishing fitness for purpose is formal validation. This assists with demonstrating the integrity and value of the underlying technology.

5.11 Validation is 'The process of providing objective evidence that a method, process or device is fit for the specific purpose intended'[101]. It involves demonstrating that a method used for any form of analysis is fit for the specific purpose intended i.e. the results can be relied on. It is the expectation of the Forensic Science Regulator (England and Wales) that all methods routinely employed within the criminal justice system will be validated prior to their use on live casework material.

5.12 Once a method has been validated in another organisation, there is a requirement for the organisation wishing to use this new method to review the validation records to ensure that it has been done correctly. Once satisfied, the new user need only undertake verification for the method to demonstrate that the organisation is competent to perform the test/examination, i.e. demonstrating that it works in their hands. This could be important because, in many areas, the technology is being employed by non-scientists/non-experts with no detailed understanding of the underpinning science.

5.13 The validation approach will vary depending on the nature of the method/system, the manner in which it is used and the risks to the criminal justice system. A full validation process could include the following:

1. Determination of the end-user requirements and specification

[101] Codes of Practice and Conduct for forensic Science providers and practitioners, published by the Forensic Science Regulator (England and Wales) at: www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2017

2. Risk assessment
3. Review of end-user requirements and specification
4. Set the acceptance criteria
5. Validation plan
6. The outcomes of the validation exercise
7. Assessment of acceptance criteria compliance
8. Validation report
9. Statement of validation completion
10. Implementation plan

6 Statutory Code of Practice

6.1 We recommend that a Code of Practice be established in legislation. The detail of the Code need not appear in legislation. Using the Code for aspects of oversight should allow greater flexibility when it comes to regular review by the Scottish Parliament than would be the case if relying solely on primary legislation.

6.2 Responses to our requests for submissions demonstrated support for a Code of Practice. See, in particular, the Justice Scotland submission to the IAG (paragraphs 31 to 37) and the submission from the Open Rights Group.

6.3 We suggest that the Code should be developed and finalised to come into force at the same time as the Commissioner takes office. This can be done following public consultation, as well as further discussion with relevant bodies and individuals. A more detailed outline of possible contents of the Code should be prepared ahead of public consultation on our recommendations. The Commissioner can take responsibility for matters relating to enforcement of the Code, subject to review by the Parliament.

6.4 In our discussions of a Code of Practice, we wondered about the audience for the Code. It appeared to us that a Code may have different possible audiences – the public, police, forensic practitioners, private bodies. This led to a question as to whether there should be one Code or several. A single Code might necessarily be lengthy and therefore off-putting for public consumption. To appeal to the public, however, it might have to be expressed in simpler terms than would seem useful to practitioners. Our recommendation is for a single Code of Practice, but we suggest that decisions on whether to create different versions for different audiences might usefully be made by the Commissioner. In looking at this question, the Commissioner can consider not only the different audiences but also any differences in use of different types of biometric data. In any event, there should be an easy read version of the Code.

6.5 We suggest that consideration is given to a separate section in the Code to address specific issues relating to children and others with vulnerability.

6.6 Public consultation should take place on the general principles likely to feature in the Code, which might usefully be taken from Chapters 4 and 5 of this report. It should also cover the scope of the Code, in particular, whether it should be restricted to public bodies in the criminal justice sphere, or apply to public bodies more widely, and whether it should apply also to the private sector.

6.7 The relationship between the Commissioner and private bodies should be consulted upon. Private bodies are responsible for a large and increasing amount of biometric data. It is arguable that they should come under public regulation and not merely be allowed to rely on contractual arrangements with their customers/clients. One suggestion was that public contracts should only be awarded to private bodies that

were ‘accredited’, i.e. that adhered to the Code of Practice. The consultation can address this point.

6.8 Transparency and accountability are vital to ensure ongoing public trust and to adhere to basic democratic and rule of law principles. The Commissioner should be required to make information publicly available about biometric data acquisition, retention, use and deletion. This should include quantitative and qualitative information, including any relevant Key Performance Indicators. There should be an obligation on bodies to publish and explain data on their biometric data retention and use. We discussed whether this obligation should be restricted to all, or specific, public bodies or include private bodies. This can be the subject of consultation, but our view is that the obligation should extend also to private bodies.

6.9 The Code could specify any other implications of non-compliance (for example in relation to internal disciplinary procedures). That too should be the subject of consultation.

6.10 If, contrary to our recommendation, there is a presumption for retention of biometric data on the expiry of retention periods, the Code should specify procedures for application for deletion. This should include issues of accessibility, including easy read material, fees, advice and assistance. Even with a presumption for deletion, similar provision would be needed for individuals whose data was retained for specific reason despite the presumption.

Courts

6.11 It seems likely that there may be more proactive management of cases by the judiciary. This could include an earlier and more interventionist role in assessment of the reliability of biometric technologies and science, as part of the Court’s task in determining the admissibility of evidence. This would help to keep a balance, allowing innovative but unvalidated science to be used as an investigative tool, but maintaining a harder line when it comes to assessing what is admissible evidence.

6.12 Breaches of the Code will not be conclusive for the purposes of admissibility but can be taken into account by the Court in determining admissibility.

6.13 Breaches of the Code should not of themselves constitute a civil or criminal offence.

Recommendation 2

Legislation should establish a Code of Practice covering the acquisition, retention, use and disposal of DNA, fingerprints, facial and other photographic images (including custody images) and all existing, emerging and future biometrics for Police Scotland, the Scottish Police Authority and other bodies working in the field of law enforcement. The legislation should outline matters relating to review of the Code by the Scottish Parliament.

Recommendation 3

The Code of Practice should be the subject of detailed consultation. It should contain relevant human rights and ethical principles, address the implications of any presumption regarding retention and specify relevant procedures for applications from private citizens for deletion of biometric data. It should contain specific reference to validation of biometric technologies.

7 Children

7.1 For obvious reasons, this is an area deserving of special attention given that there is currently no separate set of policies or practices as regards biometric data obtained from children and young people. To that end, we established a Sub-Group to look specifically at whether special provisions should be introduced for children. We consulted with young people and those working with children and young people, as well as police officers specialising in this area.

7.2 For our purposes, we have adopted the United Nations Convention on the Rights of the Child definition of children as being those under 18. We have focussed primarily on children aged between 12 and 17 although we will mention the position regarding those under the age of criminal responsibility (which will increase from eight to 12 in terms of the Age of Criminal Responsibility (Scotland) Bill).

7.3 The numbers of children who come into contact with the police is relatively small in comparison to adults and, over the last decade in particular, it has reduced significantly (at least partially as a result of changes to the way in which children and young people involved in offending are dealt with by diversionary measures). As discussed earlier, only around 2,200 children were proceeded against in the Scottish courts during 2015/16, of whom very few were under the age of 16. More children are dealt with through the Children's Hearings system – in 2016/17, there were 26,840 referrals to the Children's Hearings system, of which 73% were on a non-offence (care and protection) basis and only 27% on offence grounds.

7.4 This provides reasonable justification for taking an appropriately distinct approach to the capture of their biometric data. Such an approach is also required by relevant legislation and human rights considerations. It is recognised that biometric data are not required in every case involving a child. In some areas of policing, individual decisions are based on an individualised risk assessment on a case by case basis and it is the view of the Group that a similar approach would be suitable for the acquisition, retention, use and disposal of biometric data as it relates to children.

7.5 Police officers who deal with children and young people on a regular basis are well aware of the issues around criminalising children. They work with the aim of keeping children out of the formal justice system as far as possible, in a manner consistent with, and supported by, the Whole System Approach[102]. They are also mindful of the risks of stigmatising children through labelling practices which are often driven by evidence of 'previous form' rather than current behaviour. For these reasons, there is a strong need to ensure that biometric data are acquired, used and retained in a

[102] http://www.gov.scot/Topics/Justice/policies/young-offending/whole-system-approach

proportionate manner that reduces any unintended negative risks or consequences for the individual.

7.6 This is important and should be reflected in the legislative approach to the retention of biometric data of children. As indicated in Chapter 2, there is a three year retention period for biometric data where grounds of referral are established (whether through acceptance by the child at such a hearing or a finding at court) in relation to a prescribed sexual or violent offence but the possibility of indefinite retention if a child is convicted of any offence at court. This legislative distinction seems anomalous but may be justified in particular cases. It should be reviewed in light of any evidence which becomes available. We make appropriate recommendations in Chapter 8 in relation to the review of retention periods generally, but also those relating to children.

7.7 For children under 12 who, under the Age of Criminal Responsibility (Scotland) Bill, will no longer be capable of being held criminally responsible, certain biometrics will not be obtained except where they are needed for the investigation of a very serious incident. Under the Government's proposals, the capture or use of biometrics will have to be authorised by a Sheriff and biometric data taken from children under 12 will have to be destroyed as soon as they are no longer needed for the specific investigation and any ensuing Children's Hearing proceedings – they will not be placed on the CHS or PND.

7.8 To assist with context, it should be noted that, in the last three years, only three children (all aged 11) have had biometric data captured and placed on the relevant database. In these circumstances, we do not consider it necessary to make any recommendations applicable to this group as the specific circumstances of each child and case will be considered each time, subject to judicial oversight.

7.9 For children aged 12 to 17 years, Police Scotland accept that, in each case, consideration should be given by the relevant officer as to whether it is proportionate and necessary to obtain biometric data for the purposes of recording on the biometric databases, with the best interests of the child specifically taken into account in the decision-making process. In doing this they should consider the wider context of the child's offending behaviour, including their previous offences, their likelihood of reoffending and the nature and seriousness of their offending behaviour. Where the decision is to obtain and retain biometric data, the relevant officer should record the reasons. These reasons should be subject to review and scrutiny within a reasonable timeframe, both internally by supervising officers and by the Scottish Biometrics Commissioner.

7.10 We recommend that this should be the new approach for children in this age group. The legislation and Code of Practice should reflect that commitment. This approach would be consistent with the 'Getting it Right for Every Child'[103] framework and the 'Whole System Approach' for young people who offend. This forms the current ethos of Scottish youth justice policy.

7.11 Where formal measures are taken, a majority of cases involving children may be referred to the Children's Hearings system, but we see no reason for present purposes to distinguish between children based on whether their cases are dealt with through the Children's Hearings system or the courts. The approach to the capture and retention of biometric data for all children aged 12 to 17 should be the same and should remain distinct from the approach to the biometric data of adults.

7.12 Of note, in our meeting with two Members of the Scottish Youth Parliament, the issue of awareness was raised as a priority. They noted that the 'retention period is less important [to young people] than awareness of rights regarding applications for deletion/challenge to extensions' [quote from Member of Scottish Youth Parliament]. This highlights the issues raised in Chapter 8, below, on periods of retention; however, it is of particular relevance here given the general lack of knowledge amongst the Scottish public about their rights with regards to biometric data (considered above in Chapter 3) and the fact that this is likely to be exacerbated amongst children and young people.

7.13 In the interim period before any new legislative provisions take effect, we encourage Police Scotland and the SPA to review existing policy on children (voluntarily) in light of the IAG report.

7.14 If there are any processes introduced which depend on awareness, consent or meaningful participation, care should be taken to ensure that suitable adaptations are made, having regard to the vulnerability of the particular individual.

[103] http://www.gov.scot/Topics/People/Young-People/gettingitright

Recommendation 4

Distinct policies should be formulated for the acquisition, retention, use and disposal of the biometric data of children aged between 12 and 17. In each case involving a child, consideration should be given to the proportionality and necessity of obtaining biometric data for the purposes of recording on the biometric databases, ensuring that the best interests of the individual child are taken into account in the decision-making process. Where the decision is to obtain and retain biometric data, the reasons should be recorded and subject to review and scrutiny. Appropriate consideration should be given, and adaptation made, in the treatment of the data of those (children and adults) with specific vulnerabilities.

8 Retention Periods

8.1 Members of the public and those involved at Police Scotland and the SPA should have greater clarity about retention periods. Subject to anything learned from evidence which becomes available in the future, these periods should be the same for all biometric data even if it is kept in different databases. On present evidence, which is extremely limited, there seems to us to be no justification for different retention periods across different types of biometric data. That raises the question of what is an appropriate retention period. The best answer is probably a period specific to the various factors relating to the particular individual and any offending or alleged offending, taking account of prior criminal history, outstanding allegations and risk assessments. Although appropriate and manageable in relation to children, such a case-specific approach would undoubtedly be unduly burdensome when it comes to the majority of cases.

8.2 Current retention periods, indefinite and specific, are essentially arbitrary – there is little or no evidence to support any particular period. The requirements around transparency and accountability, as discussed in Chapter 4, 5 and 6, should assist in determining if we can better identify appropriate periods. Current retention periods, although contained in primary legislation, should be reviewed and, thereafter, kept under review along with the Code of Practice. This should be done on the basis of consideration of such evidence as is, or becomes, available, in Scotland and elsewhere. It may not be possible to specify a particular period for ongoing review, as it should relate to the availability of suitable evidence. Specifically, we have in mind evidence about the value of biometrics in the investigation of certain offences, re-offending rates relating to different crimes, the escalation of offending, and the value that biometric retention has in the investigation of this escalation. In assessing the value of biometrics in the investigation of certain offences, the experience of police officers, prosecutors and others will be of assistance. Scope for this level of discrimination in retention policies has been recognised, for example, in the 2016 report of the UK Biometrics Commissioner which states:

8.3 ‘For some crimes biometrics are often of importance in identifying the offender (e.g. burglary[104]), for others they may be (e.g. rape) and others rarely (e.g. domestic violence) [105].’

8.4 It occurs to us that the Risk Management Authority may have evidence or insight to offer in relation to matters relevant to determining appropriate retention periods. This could be explored by the Commissioner in due course.

---

[104] ‘housebreaking’ in Scotland.

[105] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644426/CCS207_Biometrics_Commissioner_ARA-print.pdf at paragraph 123.

8.5 It is possible also that some evidence of the type we suggest will become available through the work of the UK Biometrics Commissioner. In England and Wales, Chief Officers of Police can apply to the UK Biometrics Commissioner to retain the biometrics of people, with no prior convictions, who have been arrested for a 'qualifying offence'[106] but neither charged nor convicted. The police must persuade the Commissioner that retaining the biometrics will be useful in the detection, prevention or deterrence of crime. Since the relevant sections of the PoFA came into force on 31 October 2013 to 31 December 2016, 386 such applications to the Commissioner were received. Biometric material held following a successful application to the Commissioner has only recently come to the end of the initial three year retention period. The UK Biometrics Commissioner has mentioned the possibility of relevant evidence from this aspect of his work:

8.6 'Since the first applications to the Commissioner…to be approved were in relation to material taken in November 2013, over the coming months and going forward it is my intention to examine the rate of conviction for subjects during the 3-year period that their biometrics are retained[107]. '

8.7 For the avoidance of doubt, we do not suggest replicating any other existing procedure in England and Wales, merely looking there for relevant evidence or guidance as to an appropriate approach to the retention of biometric data.

8.8 Currently, retention periods vary between two or three years (subject to extension on review) to indefinite retention. Attempts to refine rules on data retention, particularly those which permit indefinite retention, are appropriate, not only on a human rights basis but also because '…over time limitless retention of records would inevitably clog the databases with biometrics of no further utility at increasing expense to the tax-payer…[108]'

8.9 There is no evidence enabling us to make any recommendation about the appropriateness or otherwise of current retention periods. Such evidence should be sought and considered as part of ongoing review. In the meantime, it cannot be said that current determinate periods are incorrect or unjustified. They also coincide with equivalent periods in England and Wales.

---

106 Generally more serious violent, sexual offences, terrorist offences and robbery. Police and Criminal Evidence Act 1984 (Amendment: Qualifying Offences) Order 2013.

107 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644426/CCS207_Biometrics_Commissioner_ARA-print.pdf at paragraph 133.

108 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644426/CCS207_Biometrics_Commissioner_ARA-print.pdf at paragraph 45.

8.10 The picture can be kept under review by the Commissioner in light of any evidence.

Areas for review

8.11 Indefinite retention: The proportionality of indefinite retention of biometrics of all convicted persons, with no differentiation reflecting the gravity of offence, is to be considered by the ECtHR in the case of *Gaughran*. Notwithstanding the decision of the UK Supreme Court, discussed in Chapter 4, it is questionable whether such a blanket policy is proportionate, and consideration should be given to amending the current approach. It appears to us that there should at least be a review of the current indefinite retention rules based on a single conviction, taking account of any emerging changes in jurisprudence, whether in Scotland, England and Wales, or at the ECtHR. To whatever extent is currently possible, and certainly in relation to ongoing review, this should be research led and consider not only the gravity of the offending but also the value of biometrics in the investigation of certain offences, re-offending rates relating to different crimes, the escalation of offending, and the value that biometric retention has in the investigation of this escalation.

8.12 Children: Review of retention periods should also extend to those applicable to children's data. If, however, an individualised approach is adopted for the retention of each child's data, regardless of whether proceedings are taken at court or through the Children's Hearings system, as suggested in Chapter 7, this may not arise. Otherwise, there should be a review of retention periods as they relate specifically to children, including the three year retention period where grounds of referral are established (whether through acceptance by the child at such a hearing or a finding at court) in relation to a prescribed sexual or violent offence and the possibility of indefinite retention if a child is convicted of any offence at court.

8.13 Fiscal offer/Fixed penalty: There should be consideration of differentiation in the length of data retention when someone has chosen to accept a disposal e.g. a fiscal offer or police fixed penalty, as opposed to those who do not and who are then not convicted. It is important to recognise that such offers/penalties do not operate on the basis of a requirement for formal acceptance. They operate by way of presumption that they are accepted unless challenged. If disputed, the individual must therefore take formal steps to challenge the penalty. There is a disparity here, and it is unlikely that all of those who 'choose' to accept such an offer or penalty are aware that they are doing so, or of the full implications of inaction. Retention of biometric data in such circumstances should be reviewed, and public awareness raised around the issue. To whatever extent possible, this review should also be research led and consider the matters referred to above in relation to indefinite retention.

8.14 In summary, the Government should consider reviewing sections 18 to 19C (excluding section 18G which relates to reserved matters) of the Criminal Procedure (Scotland) Act 1995 in relation to:

- Potential indefinite retention of biometric data following conviction

- Retention of biometric data of children (see Chapter 7)
- Retention of biometric data subsequent to a fiscal offer or fixed penalty.

8.15 To complete the review of these sections, the definition of 'relevant physical data' in section 18(7A) of the 1995 Act should be expanded so that it is wide enough to include all existing, emerging and future biometric technologies. While DNA, fingerprints and photographic images involve familiar technologies, such a new definition would allow for others, including some which have not yet been developed. Expanding the statutory definition is consistent with the idea of establishing a legislative and ethical framework for regulation and oversight in this area which will be able to adapt to new technologies in a way which improves public protection while safeguarding human rights. The expanded definition should not be used to allow the capture, storage, retention, use and disposal of biometric data using emerging and future technologies in regular policing practice until they have addressed the matters referred to in our section on validation in Chapter 5. One means of addressing this would be to stipulate that, before any other type of biometric samples could be taken, there would require to be legislative approval following consultation. To avoid unnecessary delay, such approval could be given by way of statutory instrument rather than amending the 1995 Act. Secondary legislation made under a new delegated power in the 1995 Act could be subject to the affirmative procedure in Parliament, which would mean the legislation would have to be approved by Parliament before it came into force. Provision might also be made for the Commissioner to trigger an ad hoc investigation and report that would be laid before, and considered, by Parliament. That way any statutory instrument would still be subject to broader consideration. This would help to ensure proper oversight, scrutiny and flexibility, without blocking technological progress of benefit to the public.

Presumption in favour of deletion

8.16 In view of the fact that data retention is an interference with the right to privacy, the obvious approach is to have a presumption in favour of deletion following the expiry of any minimum retention period. On this point, see also paragraph 2.8 of the submission to the IAG by No2ID Scotland and pages 14/15 of the submission by the Open Rights Group.

8.17 We acknowledge that public protection is a relevant factor to be considered in looking at the question of a presumption.

8.18 We recognise, also, that a presumption for deletion may have practical and resource implications. It has not been possible to ascertain, or even estimate, the likely greater costs associated with our recommendation of a presumption in favour of deletion. No doubt, the Government will wish to obtain accurate costings of the two alternatives. It may be that some of these costs will be addressed more easily with the new National Custody System.

8.19 If the presumption is for deletion, there would still have to be a procedure to allow individuals to apply for deletion where a decision was made to retain their data notwithstanding the presumption. Likewise, in the event of a presumption in favour of retention, there would need to be a procedure to allow individuals to seek the deletion of their biometric data.

8.20 Any such procedures would involve a level of bureaucracy and expense, as well as requiring far greater public awareness of this area, including any rights to apply for deletion. It may be worth consulting on this aspect, including views on assistance for individuals to navigate the process, especially for children and vulnerable individuals. There may also be a question as to whether fees should be payable. If there is to be such a system, it should be arranged to ensure maximum opportunities for individuals to use it, undeterred by complexity or cost.

8.21 There needs to be greater public awareness of the position regarding retention. Police officers should explain the relevant retention periods to individuals when biometric data is being captured. Consideration should be given to the best means of doing so effectively, whether by handing over brief information sheets, direction to a website, or some combination of such methods. The Commissioner should carry out work to ascertain the best means of increasing public awareness in this area as well as more generally.

Recommendation 5

There should be a review of the rules on retention of biometric data in sections 18 to 19C of the Criminal Procedure (Scotland) Act 1995, considering all questions of proportionality and necessity. The review should be research led and consider not only the gravity of the offending but also the value of biometrics in the investigation of certain offences, re-offending rates relating to different crimes, the escalation of offending, and the value that biometric retention has in the investigation of this escalation. It should be informed by any developments in the law in Scotland, England and the European Court of Human Rights.

Recommendation 6

There should be a presumption of deletion of biometric data after the expiry of prescribed minimum retention periods.

Recommendation 7

Evidence should be gathered from which continuing assessment can be made about appropriate periods of retention of biometric data. Public consultation should include specific questions on retention periods.

9 Oversight – Scottish Biometrics Commissioner

9.1 *'Changes in technology happen at a pace that the legislature fails to keep up with. This is a challenge for all Governments across the world, but it isn't insurmountable. Creating independent bodies of experts that are able to track the changes in technology, how those technologies are put into practice, and whether the legislative framework continues to serve its original purpose, is a good approach to meeting the challenges of an ever-changing technological landscape*[109]*.'*

9.2 There is currently no independent governance or oversight of the use of biometric data in policing in Scotland. This gap was highlighted in the Fraser Report in 2008 and, again, in the HMICS Report in 2016. The latter report specifically recommended the creation of a Scottish Biometrics Commissioner. There are distinct considerations in biometrics in policing which underline the need for specific scrutiny, many of which have been addressed elsewhere in this report.

The need for a Commissioner

9.3 It is instructive to consider the oversight picture for biometric data in England and Wales. There, independent oversight involves several bodies which contribute to the overall picture, with each offering different perspectives and emphasis – the National DNA Database Strategy Board[110], the UK Biometrics Commissioner, the Forensic Science Regulator (England and Wales), and the Biometrics and Forensics Ethics Group. The position there is complicated but apparently clear enough to those involved and generally well understood.

9.4 In addition, the Information Commissioner's Office (ICO) has general oversight of all personal data usage, whether of a biometric kind or not, although the new GDPR and the law enforcement provisions of the DPB do specifically highlight such data. The new data protection regime, although basically following present regulation, will give the ICO more power and will especially give more rights for data subjects to both be informed and challenge the holding of data about them. This will not necessarily change the situation as regards the PoFA and police use and holding of

---

[109] Submission to IAG from the Open Rights Group (page 4).

[110] https://www.gov.uk/government/groups/national-dna-database-strategy-board - the Strategy Board comprises representatives of the National Police Chief's Council, the Home Office, the DNA Ethics Group, the Association of Police and Crime Commissioners, the Forensic Science Regulator(England and Wales) (or her representative), the Information Commissioner's Office, the Biometrics Commissioner (or his representative), representatives from the police and devolved administrations of Scotland and Northern Ireland and such other members who may be invited.

DNA and fingerprints, but it may well mean that the police will need to be more transparent and provide a mechanism for data subjects to exercise their strengthened rights. It may have a more significant effect on those second generation biometrics outwith the PoFA and currently governed either by the England and Wales Management of Police Information Code of Practice or not at all, an area likely to be considered by the Forensic Science Regulator (England and Wales) in relation to quality aspects of the biometrics as opposed to issues relating to retention.

9.5 The UK Biometrics Commissioner liaises regularly with the ICO. It is understood that arrangements work well generally without the need for a formal Memorandum of Understanding.

9.6 The Forensic Science Regulator (England and Wales) has oversight of the scientific quality of forensic evidence and her oversight has been strengthened. Her role is clear. The UK Biometrics Commissioner liaises regularly with her and they work together on the limited areas where there is a shared interest. Currently, they are working together to try and improve the understanding and ability across the criminal justice system to use scientific evidence.

9.7 The Surveillance Camera Commissioner has responsibility for drawing up a voluntary Code of Practice for the use of public camera systems. Recently, however, he has written to all police forces saying that he has control of the use of facial imaging (because it uses cameras) and they should not use facial imaging in public places without his permission. This has caused some concern about clarity around the PoFA and the role of the Information Commissioner.

9.8 Given the presumption against the creation of new public bodies in Scotland, we considered the question of whether oversight in this area might be added to the responsibilities of an existing commissioner or public body. Having examined the various options, it appears to us that there is no body within the competence of the Scottish Parliament to which oversight in this area could readily be given. More generally, as can be seen from England and Wales, there is some overlap of responsibility with the ICO which is a UK body. Data protection is a reserved matter and therefore the ICO exercises these powers in Scotland as well as the rest of the UK, albeit with a Scottish presence.

9.9 The existence of the ICO in England and Wales did not preclude the need to establish a separate Biometrics Commissioner and, although there is some overlap, each oversees distinct areas which are widely recognised as requiring separate scrutiny. The reports and other work of the UK Biometrics Commissioner, generally accepted and welcomed by the UK Parliament, have highlighted the need for specific oversight in this complex and developing field. Finally, a majority of the responses and submissions we received supported the creation of a new body to provide independent oversight in this area.

The Commissioner's Role

9.10 Written submissions to the IAG addressed various possible aspects of the role of the Commissioner. We found these submissions helpful and quote from some here where we accept them and wish to include them as part of this report.

9.11 The Commissioner should[111]:

- have an independent complaints mechanism
- be able to begin investigations from their own mandate
- be able to develop Codes of Practice relating to the handling of biometric data, and hold bodies to account for following the rules set out
- report to the Scottish Parliament and publish findings each year of the reviews they undertake and the outcome of their investigations.

9.12 'The Commissioner should also have a large part of public education and public engagement. One of the areas the public is continually let down on is the delivery of clear, jargon free information to help them understand the powers authorities have, the powers they [the public] have to hold those authorities to account, and how to exercise those powers. A commissioner with a mission statement relating to public engagement and education would go some distance to maintaining a public feedback loop for the Commissioner, noting the shifting expectations of the public, and reacting to those changes with new guidance, or public education initiatives[112].'

9.13 Oversight by the Commissioner should extend to all aspects of policing and law enforcement subject to the competence of the Scottish Parliament. Specifically, this will include Police Scotland and the SPA, as well as any other related public bodies. The Commissioner should be able to issue guidance to public bodies in the criminal justice field, as well as offering support in their ethical use of biometric data – existing, emerging and future.

9.14 There are other areas of Government in which biometric data feature (for example, health and education), although these fall outwith our Terms of Reference. Consideration can be given as to whether the role of the Scottish Biometrics Commissioner should be extended to these.

9.15 It is, as yet, impossible to assess the scale of the role of a Biometrics Commissioner in Scotland. Ideally, in terms of recognised good practice for such bodies, it may be

---

[111] Submission to IAG from the Open Rights Group (page 19).
[112] Submission to IAG from the Open Rights Group (page 18).

that there would be a commission rather than a singleton commissioner[113]. This was put to us in written submission. On the other hand, we recognise that a Commission might seem disproportionate in the Scottish context given that we have only a single primary Scottish police service as opposed to the 43 constabularies that are subject to scrutiny in this area by one part-time UK Biometrics Commissioner. The size of the population and the amount of biometric data is also relevant, although we see the role in Scotland developing and increasing with advances in related technologies. The Commissioner can keep the Scottish Parliament advised on their ability to offer meaningful oversight and scrutiny.

9.16 Public consultation can consider the role, powers and functions of the Commissioner in parallel with consultation on the potential content of a Code of Practice. This should include the suggestions in this chapter.

9.17 The Commissioner should have powers to investigate compliance with any Code of Practice by the bodies to which it applies, making recommendations, and following up those recommendations, as well as reporting publicly on the outcomes[114].

9.18 In Scotland there is no Surveillance Camera Commissioner. One respondent suggested a commissioner whose oversight covered biometrics and CCTV where biometric data can be captured without knowledge or consent. This area extends beyond our Terms of Reference, and we make no recommendation, but it is a matter which can be considered in due course. It could also be the subject of consultation.

9.19 On the remit of the Commissioner, see also the submission to the IAG from the Open Rights Group (pages 17/18).

Ethics Advisory Group

9.20 As will be apparent from previous Chapters, biometrics and biometric data in policing are areas with significant ethical issues, challenges and concerns. In recognition of this, some work is already being done to promote specific consideration of ethical issues within Police Scotland and the SPA.

9.21 In this area, we have been impressed by the contribution in England and Wales of the Biometrics and Forensics Ethics Group. The BFEG has 13 members. Although it has only four plenary meetings annually, much work is done through sub-groups. It

[113] House of Lords Constitution Committee, in its 2004 report 'The Regulatory State: Ensuring its Accountability' - https://publications.parliament.uk/pa/ld200304/ldselect/ldconst/68/6803.htm - see recommendation 3.

[114] Submission to IAG from the Open Rights Group (page 19).

produces an annual report. Its last report[115], published on 30 October 2017, includes updates on its work in 2016:

- the use of next generation sequencing technologies
- a pilot project on the international exchange of DNA
- the development of a set of high level ethical principles for stakeholders
- the retention and use of custody images
- the role of forensics in achieving criminal justice outcomes
- developments in rapid DNA and Y-Short Tandem Repeat technologies
- ground-truth databases
- DNA paternity testing for child maintenance cases

9.22 We recommend that there should be an Ethics Advisory Group on Biometrics in Scotland. This Group can support, test and challenge the Commissioner and other relevant bodies. Liaising with others working in relevant areas of ethics, the Group will offer advice on options as to how, or whether, to proceed with proposed developments in technology. We see considerable scope for liaison with the BFEG, possibly to include observers from each Group attending meetings of the other.

9.23 It seems to us that there are individuals in Scotland, especially in our universities, who would be ideal to perform such a role. We received considerable assistance from them and, whether or not directly involved in such a Group, we are confident that they would have a useful role to play in the oversight landscape, especially when we are recommending greater transparency and evidence-gathering.

9.24 Some additional scoping work might usefully be carried out in advance of public consultation to explore various options for the establishment of such a Group and appointment of its members. We thought it useful to look at the requirements for BFEG members which include full compliance with the requirements of the Office of the Commissioner for Public Appointments. Appendix 8 contains the information published last year when the BFEG was seeking new members. This is included for information only, and we make no specific recommendation about the process for establishment of, or appointments to, such a body.

9.25 For the avoidance of doubt, we do not suggest replication of the full oversight regime in England and Wales.

[115] https://www.gov.uk/government/publications/national-dna-database-ethics-group-annual-report-2016 - the last report published by the National DNA Database Ethics Group before it became the BFEG on 20 July 2017.

Reporting

9.26 The Commissioner should report annually to the Scottish Parliament. The Commissioner should be responsible for publication of a report. Periodic review by the Parliament should be at regular intervals, perhaps every three to five years. Earlier review might be appropriate in the early stages of the new oversight regime but that would be a matter for the Parliament. In addition, it should be possible for a review by the Parliament to be requested by specified bodies or office-holders, specifically the Scottish Biometrics Commissioner, the Cabinet Secretary for Justice, the Lord Advocate, the Chief Constable of Police Scotland, the Board of the SPA, HMICS and the Police Investigations and Review Commissioner.

> 'The Commissioner's mandate should involve giving expert evidence in policy deliberations that are within its remit. This helps to ensure the relevance of the Commissioner and provide opportunity for regular contact between the Commissioner, the Scottish Parliament, and the public.'[116]

Support

9.27 The Scottish Biometrics Commissioner should have a secretariat. This might usefully be shared with another organisation independent of government, possibly a Non-Departmental Government Body. Alternatively, it might be based at a university. The latter possibility may have advantages when it comes to establishing an Ethics Advisory Group, for reasons outlined above.

Legislation

9.28 In addition to provisions regarding the Commissioner, legislation should also address certain other key areas.

9.29 To ensure practice in this area is in accordance with the law, data collection, processing, storage, retention, use and disposal must be governed by clear, accessible and enforceable rules set out in primary legislation and a statutory Code of Practice, and enforced by the Commissioner. Voluntary policies are not sufficient. We see a need for consistency of rules, regulations and procedures across different biometric data. Consistency will assist with compliance, as will the existence of a single regulator. At present, different policies for retention of custody images on different police databases represents a potential source of confusion. Having a single policy, based on legislation, should also assist the public in understanding their rights and obligations in relation to biometric data.

9.30 Legislation should explicitly provide for the police to take photographs and prohibit the taking of any samples other than as prescribed.

---

[116] Submission to IAG from the Open Rights Group (page 18).

9.31 Given the significance of retention periods, we suggest that these should continue to be specified in primary legislation, as is the case at present for DNA and fingerprints.

9.32 Biometrics and biometric data should be described in general terms, in the Code of Practice and primary legislation, to avoid missing a new source of data by having too narrow a definition or too exhaustive a list.

Private sector

9.33 While not involved in direct regulation of private sector bodies in this area, the Commissioner should have oversight of their work where it is done at the request of, or feeds into work by, Police Scotland, the SPA or any other relevant public body. In such cases, the relevant public body should specify a requirement on the part of the private body to comply with relevant legislation and any codes.

Recommendation 8

There should be legislation to create an independent Scottish Biometrics Commissioner. The Commissioner should be answerable to the Scottish Parliament, and report to the Parliament. The Commissioner should keep under review the acquisition, retention, use and disposal of all biometric data by the police, SPA and other public bodies. The Commissioner should promote good practice amongst relevant public and private bodies, and monitor compliance with the Code of Practice.

Recommendation 9

An ethics advisory group should be established as part of the oversight arrangements. This group should work with the Commissioner and others to promote ethical considerations in the acquisition, retention, use and disposal of biometric technologies and biometric data.

10 Miscellaneous

10.1 In the course of our work, one other matter was brought to our attention by Police Scotland. It relates to the situation where samples lawfully obtained post-conviction are of insufficient quality for use, or where samples have not been taken through oversight. The relevant power is contained in section 19 of the Criminal Procedure (Scotland) Act, 1995:

- Section 19(1)(a) – if a sample wasn't taken at time of charge
- Section 19(1)(b) – if a sample wasn't suitable for analysis (i.e. it failed to profile)

10.2 In such circumstances, another sample can be taken within the permitted period. See Section 19(4) for the permitted periods:

> '(4) In subsection (2) above, "the permitted period" means—
>
> (a) in a case to which paragraph (a) of subsection (1) above applies, the period of one month beginning with the date of the conviction;
>
> (b) in a case to which paragraph (b) of that subsection applies, the period of one month beginning with the date on which a constable of the Police Service of Scotland receives written intimation that the relevant physical data were, or the sample, was unsuitable or, as the case may be, insufficient, as mentioned in that paragraph.'

10.3 It will be seen that the current time limit for obtaining such samples, namely one month, is tight, especially as there are various administrative matters to be addressed. We understand that it is not uncommon for the period of one month to have elapsed before the request to obtain a sample finds its way to the relevant officer. In the circumstances, we suggest that the 'permitted period' be amended to three months.

Appendix 1: Membership of the Independent Advisory Group

Name	Interest/capacity
John Scott QC Solicitor Advocate	Independent Chair
Jim Fraser, Professor of Forensic Science, University of Strathclyde	Independent forensics expert
Genevieve Lennon, Chancellor's Fellow, University of Strathclyde	Law and policing
Stephen McGowan, Procurator Fiscal, High Court, Crown Office and Procurator Fiscal Service	Prosecutions/court process
Susan McVie OBE, Professor Quantitative Criminology, University of Edinburgh	Independent criminology expert
Kenneth Macdonald, head of ICO Regions, Information Commissioner's Office	Data Protection
Tom Nelson, Director of Forensic Services, Scottish Police Authority	Operation of forensic services
Derek Penman QPM, HM Chief Inspector of Constabulary in Scotland	Scrutiny of policing
Diego Quiroz, Policy Officer, Scottish Human Rights Commission	Human rights and civil liberties
Sean Scott, Detective Chief Superintendent, Specialist Crime Division, Police Scotland	Strategic and operational policing

Appendix 2: List of meetings

The Independent Advisory Group met on the following dates:

28 June 2017

18 July 2017

11 September 2017 – attended also by the UK Biometrics Commissioner, Professor Paul Wiles; the Forensic Science Regulator, Dr Gill Tully; Dr Carole McCartney of Northumbria University Law School and her PhD student, Aaron Amankwaa

26 October 2017

6 November 2017

27 November 2017

5 December 2017

9 January 2018

The Advisory Group's Children and Young People's Sub-group met on the following dates:

8 September 2017

16 November 2017 – attended also by Calum Dundas, Forensic Data Manager at National Systems Support, Police Scotland; Detective Chief Superintendent Lesley Boal QPM, Head of Public Protection, Police Scotland; Inspector Angela MacLeod, Children and Young People Business Area, Safer Communities, Specialist Crime Division, Police Scotland; Gordon Bell, Scottish Children's Reporter Administration; Juliet Harris, Together – Scottish Alliance for Children's Rights; Peter Rigg and Kit McCarthy, Members of the Scottish Youth Parliament

The following other meetings were held:

21 July 2017 – telephone call with Dr Alice Maynard, CBE; from 2006 to 2012, Alice was a Commissioner for the Human Genetics Commission.

16 August 2017 – telephone call with Professor Paul Wiles, UK Biometrics Commissioner.

24 August 2017 – meeting at Edinburgh University with Professor Robin Williams, Director of the Institute for the Study of Science, Technology and Innovation; Professor Charles Raab, Co-Chair of the Independent Digital Ethics Panel for Policing (IDEPP), member of the Data Ethics Group of the Alan Turing Institute as well as the Europol Data Protection Experts Network (EDEN), member of the Governance and Ethics Action Group in the University of Edinburgh's Internet of Things (IoT) Programme; Professor Burkhard Schafer, Professor of Computational Legal Theory; Professor Bob Fisher, School of Informatics at University of Edinburgh since 1984 and a full Professor since 2003, received his PhD from University of Edinburgh (1987), investigating computer vision in the former Department of Artificial

Intelligence, worked as a software engineer for five years before returning to study for his PhD.

29 August 2017 – telephone call with Dr Carole McCartney of Northumbria University Law School.

30 August 2017 – telephone call with Tom Vincent, Secretariat of the Biometrics and Forensics Ethics Group.

6 September 2017 – telephone call with Doctor John Innes, Leonardo; Visiting Professor at the University of Edinburgh; responsible for developing SELEX ES business – now incorporated into Leonardo - Finmeccanica since April 2016 - in the medium to long term in New Market spaces such as Critical Infrastructure Protection, Smart Cities and Mobility, Emergency Services and Healthcare; developing products, systems and services, establishing partnership and developing new business models; member of the Scottish Government's Industry Leadership Group (ILG) for the Aerospace, Defence and Marine sectors.

15 September 2017 – telephone call with Els Kindt (Post-doc legal researcher with the Centre for IT and IP Law (CITIP) of KU Leuven – iMec and leading the research line Privacy and Data Protection at CITIP; Associate Professor at Universiteit Leiden, eLaw, in the Netherlands; author of 'Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis'.

18 September 2017 – meeting with Professor Mike Nellis, Emeritus Professor of Criminal and Community Justice in the Law School, University of Strathclyde; involved between 2005-14 in the organisation of the CEP Electronic Monitoring (EM) conferences; between 2011 and 2013 acted as an expert adviser to a Council of Europe committee which drew up an ethical recommendation on EM; served on the Scottish Government's EM Working Party 2014-16; teaches Master's degree course on 'surveillance, technology and crime control' at Strathclyde.

21 September 2017 – meeting with Mike Callaghan, lead on policing issues for COSLA's Community Wellbeing Team.

26 September 2017 – telephone call into plenary meeting of Biometrics and Forensics Ethics Group.

29 September 2017 – meeting with Calum Dundas and Raymond McIntyre, both National Systems Support, Police Scotland.

2 October 2017 – meeting with Jim Wilson, Project Manager, and David Dickson, both Scottish Government Justice Directorate, Criminal Justice Delivery Unit.

10 October 2017 – meeting with Tim Ellis, Chief Executive of National Records of Scotland (NRS), Registrar General for Scotland and Keeper of the Records of Scotland, also Scottish Informatics and Linkage Collaboration (SILC); Amy Wilson, Head of Census Statistics; Gerry Donnelly, Head of Data Resources; and other NRS colleagues.

31 October 2017 – meeting with Rob Wainwright, Executive Director, and Brian Donald, Chief of Staff, both Europol

1 November 2017 – meeting with Nicola Marchant, Board Member and Tom Nelson (IAG member), both Scottish Police Authority.

9 November 2017 – meeting with Kalim Uddin, Operations Manager, Glasgow Operations Centre, Community Safety Glasgow, including demonstration of operation of CCTV in Glasgow.

16 November 2017 – telephone call with Carrie Golding, Home Office Biometrics Programme, and Alex MacDonald, Deputy Director, Biometric Quality, Home Office.

21 November 2017 – meeting with Chief Inspector Gordon Bruce (Lead) and Sergeant Iain Gibson, Criminal Justice Act Implementation Team, National Custody System (NCS) Development, Delivery and Training – meeting at Jackton, including demonstration of NCS.

24 November 2017 – telephone call with Els Kindt (see 15 September 2017).

23 January 2018 – telephone call with Dr Joanne Wallace, Head of Science and Regulatory Secretariats, Science Secretariat and Support Unit, Home Office (including responsibility for BFEG Secretariat)

Appendix 3: List of consultees

1. Genewatch UK
2. No2ID Scotland
3. Nuffield Council on Bioethics
4. Justice Scotland
5. National College of Policing
6. UK Biobank
7. Professor Dame Sue Black DBE, Professor of Anatomy and Forensic Anthropology - Centre for Anatomy and Human Identification, University of Dundee
8. Big Brother Watch
9. Open Rights Group Scotland
10. MedConfidential
11. William Perrin - Talk about Local
12. Biometrics and Forensics Ethics Group (formerly the National DNA Database Ethics Group)
13. Biometrics Institute
14. Dr John Innes - Leonardo
15. Professor Ross Anderson, Professor of Security Engineering at Computer Laboratory, University of Cambridge; Fellow of the Royal Society, the Royal Academy of Engineering, the IET and the IMA – author of “Security Engineering - a Guide to Building Dependable Distributed Systems" (http://www.cl.cam.ac.uk/~rja14/book.html)

Appendix 4: Questions to accompany the principles

The following questions are intended to clarify and aid the interpretation of the General Principles which are the foundation of the Biometrics and Forensics Ethics Group's paper which was used in drafting Chapter 5. Their purpose is also to assist those who are seeking the approval of the Ethics Group for new procedures in order to demonstrate that they have considered relevant aspects.

General Principles

Principle 1: Procedures should be used to enhance public safety and the public good

- How does the procedure enhance public safety?
- What aspect of the public good is enhanced by the procedure?
- Is there anything further that could be done to ensure that the procedure advances public safety and the public good, without unjustifiably interfering with individual human rights, e.g. the right to private life?

Principle 2: Procedures should be used to advance the interests of justice

- How does the procedure advance the interests of justice?

Principle 3: Procedures should respect the human rights of individuals and groups

- What steps have been taken to ensure that the procedure respects the human rights of individuals and groups?
- What could be done to mitigate any adverse impact on human rights?

Principle 4: Procedures should respect the dignity of all individuals

- What steps have been taken to ensure that the dignity of all individuals is respected?
- Is there any way in which the procedure could undermine the dignity of individuals? If so, how? Do the benefits of the procedure outweigh its negative side effects?
- What steps could be taken to reduce this negative impact? Could the benefit of the procedure be achieved by different means?

Principle 5: Procedures should respect and protect private life where this does not conflict with the legitimate aims of the criminal justice system to protect the public from harm

- Would the right to private life be undermined at all by the procedure? If so, in what way? Is any group or section of the community likely to be especially adversely affected?
- What steps have been taken to safeguard privacy?
- Has the appropriate balance been achieved between respecting the right to private life and public protection?
- What steps could be taken to reduce the negative impact of the procedure on the right to private life without jeopardising the procedure itself? Or could its benefits be achieved by different means?

Principle 6: Scientific and technological developments should be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims and assist the criminal justice process

- How will the procedure assist the criminal justice system by affording swift exoneration of the innocent and protection and resolution for victims?
- Is there anything that could be done to achieve these goals even more effectively?

Principle 7: Procedures should be based on robust evidence

- What is the evidential basis for the procedure?
- How has it been tested?
- Has it been subject to peer review?
- Has the evidential basis been challenged?
- What is the error/uncertainty rate?
- What are the quality control mechanisms?
- What evidence is available of the likely impact of the procedure on those to whom it is applied and any others who could be affected by it?
- Where public funds are concerned, has cost-effectiveness been considered?

Implementation of the general principles

What steps have been taken to ensure the following:

- impartiality – procedures should be applied without bias or unfair discrimination;
- proportionality – balancing individual rights and the public good;
- openness and transparency;
- the need for systems to be in place to identify errors/uncertainties;
- the need for quality control;
- the need for public accountability;
- the need for independent oversight where appropriate;
- the need to provide adequate information and, where appropriate, to obtain consent from those from whom data or samples are sought?

Considerations specific to the collection and processing of data

With respect to the collection, storage and use of data, what steps have been taken to ensure the following:

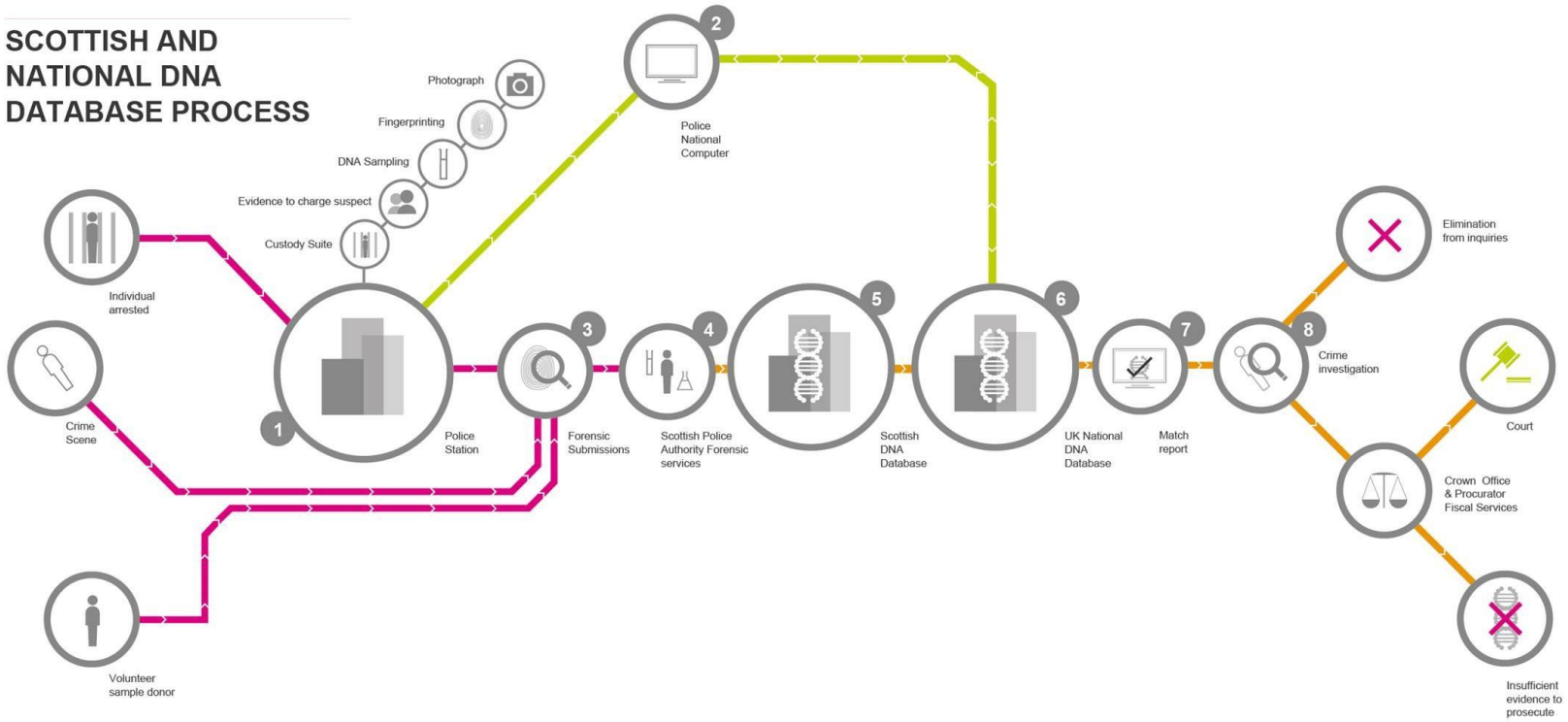
- restriction to specified and lawful purposes;
- adherence to legal requirements;
- accuracy, security and integrity of data;
- robust processes which conform to international standards and are applied by professionally trained staff;
- minimisation of intrusion into private life;
- account taken of interests of secondary data subjects, e.g. family members affected by data collection from others.

Appendix 5: Reading list

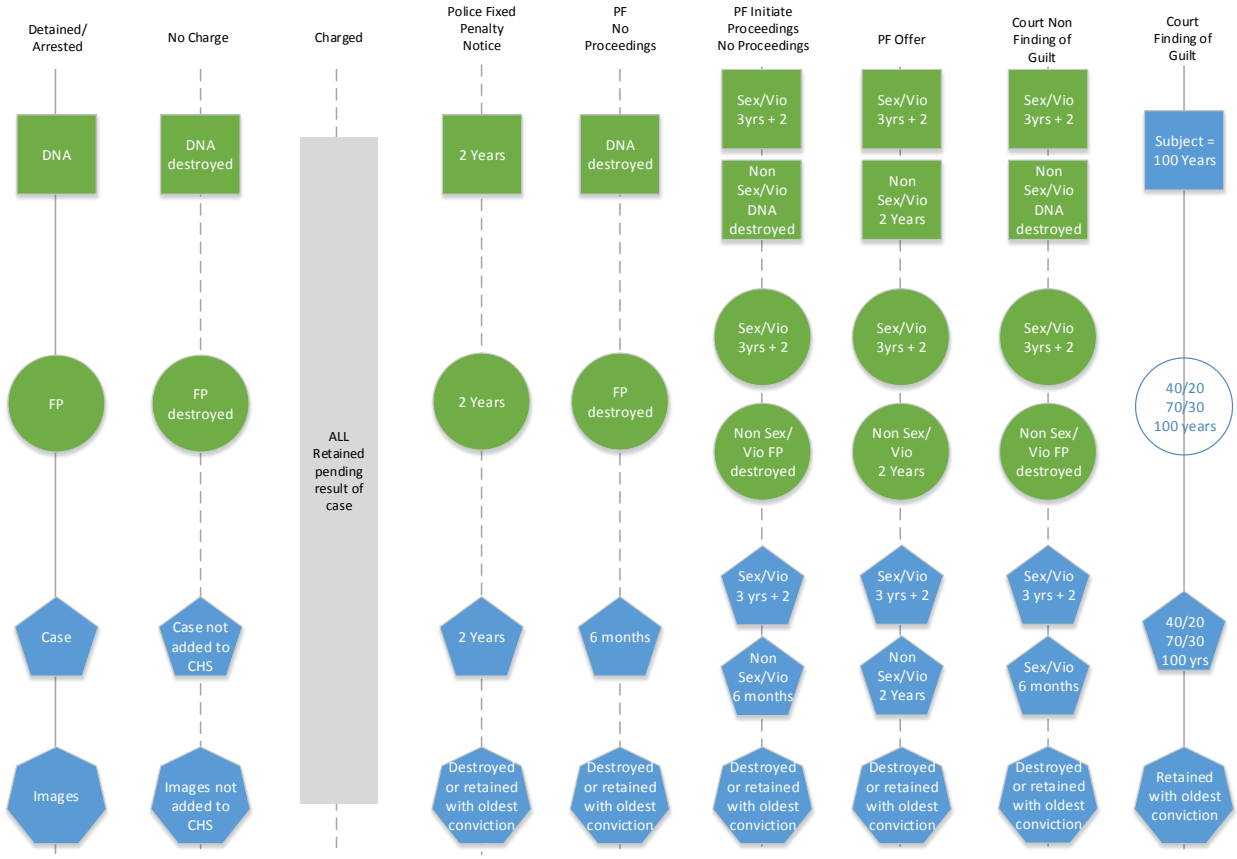
- European Court of Human Rights judgment in the case of *S. and Marper v UK*: http://www.bailii.org/eu/cases/ECHR/2008/1581.html
- The Fraser Report on Retention of DNA and Fingerprint Data and the Scottish Government response: http://www.gov.scot/Topics/Justice/law/dna-forensics/legislationscotland/reviewofprocedures
- Criminal Procedure (Scotland) Act 1995 (sections 18-20): http://www.legislation.gov.uk/ukpga/1995/46/contents
- Criminal Justice and Licensing (Scotland) Act 2010 (sections 77-82): http://www.legislation.gov.uk/asp/2010/13/contents
- HMICS report Audit and assurance Review of the use of Facial Search Functionality within the UK Police National Database (PND) by Police Scotland: http://www.hmics.org/publications/hmics-audit-and-assurance-review-use-facial-search-functionality-within-uk-police
- House of Lords and House of Commons Joint Committee on Human Rights report – Retention, use and destruction of biometric data: correspondence with Government: https://www.publications.parliament.uk/pa/jt200809/jtselect/jtrights/182/182.pdf
- Protection of Freedoms Act 2012 : http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
- House of Commons Science and Technology Committee (2015) 'Report on Current and future uses of biometric data and technologies': https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf
- Beard & Lipscombe (2015) 'House of Commons Briefing Paper on the Retention of fingerprints and DNA data'
- Scottish DNA Database Statistics: http://www.spa.police.uk/forensic-services/dna/150800/
- DNA retention for low level offending: a necessity or an overreach of police powers? MSc Dissertation, Diana Dundas, February 2015
- London Policing Ethics Panel Ethical Challenges of Policing in London: http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_-_ethical_challenges_of_policing_in_london_october_2014.pdf
- Annual Report of the Ethics Group: National DNA Database https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/568554/Annual_Report_of_the_Ethics_Group_2015.pdf
- UK Biometrics Commissioner's annual reports: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2014-to-2015; https://www.gov.uk/government/publications/biometrics-commissioners-annual-report-2015-further-report; https://www.gov.uk/government/news/publication-of-the-biometrics-commissioners-third-annual-report
- Home Office Review of the Use and Retention of Custody Images: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

- EU General Data Protection Requirements and Law Enforcement Directive: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation; http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/

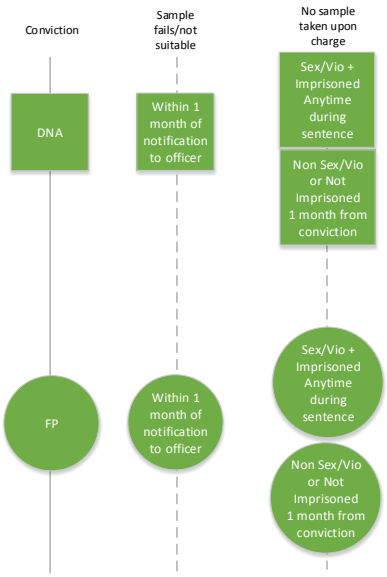
Appendix 6: Scottish DNA Database Process (adapted from Home Office: National DNA Database Annual Report 2011-2012)



Appendix 7: Police Scotland & SPA Biometrics in the Criminal Justice System Process Map (Source: Police Scotland)



Post-Conviction Sampling Powers



Note: this Police Scotland process map is intended as a guide only to assist in understanding the various complexities of retention rules. It does not illustrate the process for custody images and does not fully illustrate indefinite retention on the basis of a single conviction.

Appendix 8: Biometrics and Forensics Ethics Group Appointments Process

Centre for Public Appointments

BIOMETRICS AND FORENSIC ETHICS GROUP MEMBERS

Body:	Biometrics and Forensics Ethics Group
Appointing Department:	Home Office
Sectors:	Education, Prison & Policing, Regulation, Science & Technology
Skills required:	Change Management, Legal / Judicial, Regulation
Number of Vacancies:	9
Remuneration:	The role is unremunerated, but members will be reimbursed for travel expenses incurred whilst carrying out business on behalf of the BFEG.
Time Requirements:	10 - 15 days per year

Following a Triennial Review of the National DNA Database Ethics Group, the remit of the group was expanded to provide ethical advice on all aspects of biometrics and forensics which fall within the purview of the Home Office. This led to the establishment of the BFEG.

Committee members are expected to:

Attend and contribute to quarterly BFEG meetings, and other additional subgroup meetings arranged as necessary;

Act corporately with other members to ensure that the BFEG fulfils its responsibilities by providing Ministers and the Department with impartial, independent, balanced and objective ethical advice on issues within the group's remit.

Members also have responsibility for:

Developing the evidence base of topics under consideration to formulate advice;

Examining and challenging, if necessary, the assumptions on which advice is formulated;

Ensuring that the BFEG has the opportunity to consider the available evidence on a given issue, contrary views, and, where appropriate the concerns and values of stakeholders before a decision is taken; and

Ensuring the BFEG acts in accordance with the Code of Practice for members, which incorporates the Seven Principles of Public Life and Code of Practice for Science Advisory Committees.

Person Specification

The BFEG is seeking up to nine new members. You should have demonstrable expertise in either:

genetics, forensic science, biometric data, data protection and the ethics of consent including working with large data sets, experimental design, police service, social science, political science/political scientist, medical science or the law and be able to develop their ethical knowledge and expertise;

or

in ethics and demonstrable experience of applying this to issues across the biometric, forensic and criminal justice arena and one or more of the specialisms that underpin them.

In addition to the above your supporting statement should provide evidence of your skills and experience against the essential and desirable selection criteria set out below. Please be clear about the scale and significance of your role/achievement. The evidence you provide against the selection criteria will be used by the selection panel to determine your suitability for the role.

Essential Skills and Experience

An understanding of the breadth and depth of ethical issues related to the collection, storage and use of biometric and forensic information and data.

The ability to think logically and objectively to analyse complex information from diverse sources, identify key issues and make effective impartial and balanced decisions.

Strong interpersonal skills, including the ability to work collaboratively with committee members and stakeholders and to actively and constructively contribute to discussions, negotiating between conflicting opinions and values and generating options to reach consensus.

The confidence to deal with difficult situations sensitively, and to take and be accountable for decisions.

An appreciation of equality and diversity and a willingness to champion difference.

An awareness of how the views of the scientific community and the public are changing politically and socially.

Desirable

Evidence of working successfully in a professional, community or voluntary capacity on committees or other decision-making groups and reaching impactful and timely conclusions.

Additional Information

The successful candidate will be required to have or to obtain security clearance to Security Check (SC) level.

The Home Office is committed to providing equal opportunities for all, irrespective of race, age, disability, gender, marital status, religion, sexual orientation and transgender.

OCPA Regulated

This post is regulated by The Commissioner for Public Appointments

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-600-6 (web only)

Published by The Scottish Government, March 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS362726 (03/18)