SHRC
Scottish
Human Rights
Commission

Call for evidence

Justice Sub-Committee on Policing - the use of remote piloted aircraft systems, also known as drones, and body worn video cameras by Police Scotland

---

The Scottish Human Rights Commission was established by the Scottish Commission for Human Rights Act 2006, and formed in 2008. The Commission is the National Human Rights Institution for Scotland and is independent of the Scottish Government and Parliament in the exercise of its functions. The Commission has a general duty to promote human rights and a series of specific powers to protect human rights for everyone in Scotland.

1. The Commission would like to inform the deliberations of the Sub-Committee on this issue by providing two previous pieces of work related to the impact of the use of biometrics and new technologies in the criminal justice system. While we are not making a targeted submission on this call, we would like to share with the Sub-Committee these documents for their information. We hope these reports are useful for their discussion and scrutiny of law enforcement agencies.

2. The first paper is a human rights analysis prepared and presented to the IAG on the use of Biometrics (Annexe A) by Diego Quiroz. This paper formed the basis of the IAG Report chapter on human rights and subsequently the biometrics legislation in 2020. The second paper was prepared as a response for the Digital Strategy for Scotland last month. Both documents are in the public domain.

3. The first paper covers the key relevant human rights standards, in particular the impact of the use of biometric technology and data (as it can be derived from drone and body cameras too) on privacy (Article 8 ECHR), liberty and security (Article 5 ECHR), due process and fair trial (Article 6 ECHR). The report also covers the potential and unintended impact of the use of biometrics on our democratic freedoms (Article 9-11 ECHR).

4. The second report has a wider perspective on new technologies and offers both analysis and recommendations for future strategies in this area. Overall, the report recommends that the Scottish Government must position the protection, and realisation, of all human rights as a core principle and vision for the role of digital technologies in society. For this, it must underscore compliance with the law, including human rights law, as a key principle to ensure the protection of human rights and to prevent human rights trade-offs, and unlawful or arbitrary applications of digital technologies, particularly in key areas of life.

Annexe A

Scottish Human Rights Commission

Overview Paper for the Independent Advisory Group on Police Scotland's Use of Biometric Data

October 2017

The Scottish Human Rights Commission (SHRC) is the **National Human Rights Institution** (NHRI) for Scotland, accredited with A status by the Global Alliance of NHRIs. SHRC was established by an Act of the Scottish Parliament. It has a general duty to promote awareness, understanding and respect for all human rights and to encourage best practice. SHRC also has a number of powers including recommending such changes to Scottish law, policy and practice as it considers necessary.

SHRC is a member of the UK's National Preventive Mechanism (NPM) designated in accordance with the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (OPCAT).

Contents

I. Introduction

1. The purpose of this paper is to provide the Independent Advisory Group members with a short summary overview of the human rights legal 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).

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

3. There are both strict human rights obligations, derived from the Human Rights Act 1998, and human rights standards, emerging from international human rights treaties that would help public authorities to ensure the new framework is fit for purpose. The Equality Act 2010 sets also a number of general and specific duties for public sector organisations[1] in relation to non-discrimination,[2] which may be relevant in this area. As starting point, and recommended by the Council of Europe, the introduction and use of new technologies should take full account of, and not contravene, fundamental principles as the inherent dignity of the individual and the respect for the human body, the rights of the defence and the principle of proportionality in carrying out of criminal justice.[3]

---

[1] A private (or a voluntary) body is subject to the general duty in respect of any public functions which it has.
[2] 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.
[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

4. 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)[4] currently used by law enforcement agencies.[5] Although this point may fall outwith a strict interpretation of the Working Group's remit, the Commission notes that 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 anecdotal experiences.[6] It is also crucial to ensure that there is greater transparency and public participation around the use of biometric data in the criminal context.[7]

5. 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 this 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.[8] 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.

6. This paper is not a legal opinion, it is rather an attempt to draw out the key human rights and associated guiding principles engaged by the use of biometric data to ensure adherence to law and the greatest respect for human rights. The Commission welcomes the opportunity to

---

[4] Facial images are just the first of a new wave of biometrics.
[5] Biometrics Commissioner, annual report 2017, para 36 and Biometrics – Independent Advisory Group Review, Scotland. Big Brother Watch submission 12th September 2017.
[6] Biometrics Commissioner, annual report 2017, para 36 and Biometrics – Independent Advisory Group Review, Scotland. Big Brother Watch submission 12th September 2017.
[7] The difficult judgment as to the proper balance between public and private interest in a democratic society like ours is best taken by Parliament in the first instance, which is expressed through legislation and should not be left to the agencies using the data.
[8] See UN Guiding Principle on Business and Human Rights. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

engage with this important area and are thankful to the Chair of the Independent Advisory Group for inviting us to be part of this discussion.

II. Human Rights Law

This section discusses the impact of biometrics on human rights.

7. The Human Rights Act 1998, which incorporates the European Convention on Human Rights into UK law, sets out the fundamental rights and freedoms that everyone in the UK is entitled to. The Act has three main effects in practice:

(a) It requires all public bodies such as police, local authorities and courts, and other bodies carrying out public functions, to respect and protect the human rights in the Convention, making them justiciable in British courts;
(b) (b)It requires the courts, where possible, interpret our laws in a way which is compatible with Convention;[9] and,
(c) It sets the 'boundaries' for the Scottish Parliament's so any new legislation is compatible with the rights set out in the Convention (via the Scotland Act 1998).

8. Section 6 of the Human Rights Act 1998 makes it unlawful for a public authority to act in a way which is incompatible with a Convention right (an 'act' includes the failure to act). So, 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, as per numeral 5, and the values of the people living in Scotland.

9. Other international standards in relation to the storage and management of data include the Council of Europe Convention 108,[10]

[9] See Section 2 and 3 of the HRA.
[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Information Commissioner's Office, which is a member of this working group, would be better place to provide further detail on this area.

European Union (EU) instruments such as Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data,[11] as well as the case law of the Court of Justice of the European Union and the EU Charter on Fundamental Rights.[12] The Commission's position in relation to the EU law, as we leave the EU, is that the current legal framework should be retained. Scotland and the UK should be a global leader in equality and human rights and adopt best practice that enhances the existing protections.[13]

Article 2 of the European Convention on Human Rights and the Obligation of the State to Protect the Right to Life

10. Article 2 of the European Convention on Human Rights (ECHR) 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.

11. The fundamental nature of Article 2 is also clear from the fact that it is "non-derogable": it may not be denied even in "time of war or other public emergency threatening the life of the nation" – although, a person's right to life is not breached if resulted from a lawful act as described in para. 2 (e.g. the police uses lethal force to stop a person carrying out unlawful violence). Nonetheless, the force used must be absolutely necessary and strictly proportionate.

---

[11] 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.
[12] See e.g. Arts. 7 and 8.
[13] See more here: http://www.scottishhumanrights.com/media/1727/brexit-position-statement-december-20-dec-2016.pdf. Some of the key human rights protections and remedies coming from EU law include privacy and data protection.

12. Article 2 is relevant to several aspects of State power and provides a framework for the prevention and prosecution of homicide and the use of lethal force by the State through the mobilisation of its police and armed forces to combat terrorism, fight crime and control civil unrest.

Article 8 of the European Convention on Human Rights

13. The Commission acknowledges that the acquisition and retention of biometric information play a role in criminal justice policy and practice. However, such practices have the potential to engage the reasonable expectation of privacy that people have.[14] 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.

14. A right to protection of an individual's private sphere against intrusion from others, especially from the state, was laid down in an international legal instrument for the first time in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life. The UDHR influenced the development of other human rights instruments in Europe - and other parts of the world.

15. Article 8 of the ECHR and the Human Rights Act 1998 requires respect for private and family life, home and correspondence. These concepts are sometimes indistinguishable and cover both the protection of the moral and physical integrity of the individual. Article 8 therefore encompasses a wide range of issues. Biometric data can encompass a significant amount of sensitive information about an individual's identity, including information about their health[15] and their unique genetic code.

---

[14] Ibid

[15] 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

16. In *S and Marper v the UK*, the European Court of Human Rights (EtCHR) expressed 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"*. [16]

17. 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*."[17]

- 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*'.[18]

- 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*

[16] *S and Marper v the UK* (Applications nos. 30562/04 and 30566/04).
[17] Ibid
[18] See *Khan v the UK* Application No 35394/97 (ECHR)

sufficient."[19] In terms of assessing proportionality, three main issues are relevant:

a) the degree of the interference ,

b) whether there were less intrusive means available, and

c) the procedural safeguards available.

18. 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 his consent.

While it is relatively clear in relation fingerprints that is not the case for other biometric information. The use of facial biometrics and facial biometric recognition systems, which is used for intelligence/investigative purposes, is far more intrusive than CCTV, and can be taken without knowledge. 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. [20]

[19] As above in footnote No. 8

[20] 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.

A police photographer takes images of protesters at a climate change rally in London, December 2008. Photograph: Ashley Cooper/SpecialistStoc/REX

Source: The Guardian, available at https://www.theguardian.com/world/2017/sep/13/watchdog-warns-over-police-database-of-millions-of-facial-images accessed 28 September 2017.

19. 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 include *R (RMC and FJ) v MPS (Metropolitan Police Service)*[21] - where the court held that the retention of the custody photographs amounted to an unlawful interference with R's and F's Article 8 rights - and the Strasbourg jurisprudence emerged from a British case (*S v Chief Constable of South Yorkshire and Marper v Chief Constable of South Yorkshire*).[22] 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*

[21] [2012] EWHC 1681 (Admin)

[22] *R (on the application of S) v Chief Constable of South Yorkshire' and 'R (on the application of Marper) v Chief Constable of South Yorkshire'* [2004] 1 WLR 2196, [2004] 4 All ER 193

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".[23]

20. 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.[24] 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.*"[25]

21. A key consideration is the length of time data is stored. Useful guidance can be found in *S and Marper* and the Committee of Ministers' Recommendation No. R (92)1 and R 87 (15)[26] 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.

---

[23] Article 40 of the CRC, for example, sets out children's rights in the criminal legal system. The Commission has a statutory duty not to duplicate, so it will refrain from providing comments on children and young people in this paper.
[24] See *Evans v. the United Kingdom* Application No. 6339/05 (ECHR)
[25] see *Dickson v. the United Kingdom* Application No. 44362/04, (ECHR)
[26] Recommendation No. R 87 (15) to member states regulating the use of personal data in the police sector.

22. 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 constitute an unjustified interference with the right to respect for private life, in violation of Article 8 of the ECHR.[27]

23. It is worth noting that in the obiter dicta of *S and Marper,* the ECtHR praised Scotland for the choice of time limits on retention of DNA. The ECtHR indicated that the indefinite retention of the DNA of even convicted persons was not acceptable as a blanket policy.[28] There are also questions in relation of what convicted means e.g. cautions, reprimand and final warnings and the proportionality to retain their data indefinitely. This ECtHR decision requires the UK governments to give detailed consideration in relation to other biometric technologies they use and are planning to use (including facial images) which must meet Convention requirements. The Commission stresses the need for cogent evidence to justify retention of biometric information for both the convicted and the un-convicted.

24. One of the key points under human rights is that biometric data constitute personal data. As a consequence any policy and legal framework for its use[29] must be consistent with the human rights framework, and other guarantees laid down by relevant data protection laws.[30] The use of personal data is sensitive and must be highly protected from abuse and arbitrariness.[31] In this light, good governance

---

[27] R (RMC and FJ) v MPS (Metropolitan Police Service) [2012] and R (on the application of S) v Chief Constable of South Yorkshire' and 'R (on the application of Marper) v Chief Constable of South Yorkshire' [2004] 1 WLR 2196, [2004] 4 All ER 193

[28] See Ethics Group: National DNA Database (2009) Annual Report, p. 15 available at http://www.statewatch.org/news/2009/sep/uk-home-office-ethics-group-dna.pdf

[29] Use includes collection, capturing, retention and deletion of records for those who are found innocent or are not convicted of a criminal offence.

[30] See Data Protection Act 1998.

[31] Hammaberg, T (2008), More Control is Needed of Police Databases. Human Rights in Europe, Viewpoints by the Commissioner for Human Rights

and complaint mechanisms are supplementary and necessary safeguards against arbitrariness.[32]

Impact on Other Human Rights

25. The use of biometrics by law enforcement agencies engages a number of other human rights beyond Article 8 of the European Convention of Human Rights. 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 European Convention of Human Rights)
- The right to liberty and security (Article 5 of the European Convention of Human Rights)
- Due process and the right to a fair trial (Article 6 of the European Convention of Human Rights)
- Freedom of expression and association (Article 10 and 11 of the European Convention of Human Rights)
- Freedom of Religion (Article 9 of the European Convention of Human Rights)
- The principle of non-discrimination (Article 14 of the European Convention of Human Rights)

26. 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.

[32] This also relates to point 2 of the Group remit.

Article 3 - Prohibition of Inhuman, Degrading Treatment or Punishment

27. The absolute prohibition of torture and inhuman or degrading treatment or

punishment, enshrined in Article 3 of the European Convention of Human Rights, is so fundamental that it has no limitations or exceptions. Article 3 of the Convention is an absolute right. This means that once it has been determined that certain treatment amounts to inhuman or degrading treatment, it can never be justified. Article 3 operates differently to other rights, like Article 8 for example, which allows interferences with the right when it is justified.

28. A possible scenario in this context is the use of force by relevant authorities to obtain biometric data e.g. fingerprints. All use of force that is excessive and has not been made strictly necessary by a person's own conduct diminishes human dignity and hence amounts to inhuman or degrading treatment or punishment as prohibited by Article 3 of the Convention. Actions that cause feelings of fear, anguish or inferiority capable of humiliating and debasing a person are always prohibited by Article 3. In assessing whether the conduct by a public authority attains a minimum level of severity to come within the scope of Article 3, attention must be paid to all surrounding circumstances.

29. The use (e.g. collection) of biometrics must not amount to inhuman or degrading treatment or punishment – this is treatment which causes severe mental or physical harm or which is grossly humiliating and undignified.

Article 5 – The Right to Liberty and Security

30. Police officers are given significant amounts of discretionary power to prevent and to investigate crime, which includes pre-trial detention and administrative detention and control orders. Many of these powers are highly intrusive, particularly the powers to detain a suspect and to search for evidence. A plausible scenario that engages Article 5 of the European Convention of Human Rights is the deprivation of liberty to

obtain fingerprints or other biometric data from an individual.[33] In this case, it is imperative that any consideration to deprive a person of their liberty gives due consideration to the procedural and substantive guarantees articulated under Article 5.[34]

31. There are three aspects to the rights under Article 5. First, there is an exhaustive list of circumstances in which a person can be lawfully deprived of his liberty (paragraphs (1)(a) to (f)). Second, there is a list of procedural safeguards to be met accompanying those permissible grounds on which a person can be deprived of his liberty. Third, a person who is unlawfully deprived of his liberty has an enforceable right to compensation for that deprivation. The underlying aim of Article 5 is to ensure that no one is deprived of his liberty arbitrarily. An exhaustive examination of all those issues is beyond the scope of this paper. This protection is applicable in the context of criminal proceedings, as well as other areas in which the State might affect the liberty of persons. Not all of the grounds in Article 5 will be of relevance to biometrics as the text is designed to cover the whole range of circumstances in which State officials may feel compelled to deprive an individual of his liberty.

32. It is particularly important to ensure that children and other vulnerable individuals such as suspected victims of torture, sexual or gender-based violence, victims of other serious crimes, and/or traumatised people are protected by additional safeguards. These safeguard could include: an appropriate adult being present when a

[33] Under Eurodac Regulation (EU) No. 603/2013, all asylum seekers and migrants in an irregular situation apprehended in connection with an irregular border crossing – except for children under the
age of 14 years – must provide their fingerprints.

[34] It could be also the case that law enforcement agencies use force to obtain biometric data e.g. fingerprints. All use of force that is excessive and has not been made strictly necessary by a person's own conduct diminishes human dignity and hence amounts to inhuman or degrading treatment or punishment as prohibited by Article 3 of the Convention. Actions that cause feelings of fear, anguish or inferiority capable of humiliating and debasing a person are always prohibited by Article 3 of the ECHR. In assessing whether the conduct by a public authority attains a minimum level of severity to come within the scope of Article 3, attention must be paid to all surrounding circumstances.

vulnerable person is asked for their prints, access to a lawyer and a doctor and notification of custody, humane conditions therein as well as an strict limited duration of the depravation of liberty.

33. Controversial measures of crowd control such as kettling should be avoided when used for collecting or taking of biometric data (e.g. facial recognition) in public places. Collecting biometric data while people are engaging in peaceful assembly and association would not only stifle legitimate freedoms, but potentially engage Article 5 as it is characteristically arbitrary. It also undermines the basic principle of policing by consent.

Article 6 - Due Process and the Right to a Fair Trial

34. Article 6 of the European Convention of Human Rights guarantees that everyone charged with a criminal offence is entitled to certain protections, including the right to be presumed innocent until proven guilty, the right to a hearing with due guarantees and within a reasonable time, by a competent, independent and impartial tribunal, and the right to have any conviction and sentence reviewed by a higher tribunal satisfying the same standards.

35. As mentioned before, law enforcement officers play a key role in the task of investigating allegations of criminal behaviour. This includes a number of activities beyond detention such as interrogating suspects and witnesses, carrying out searches, undertaking surveillance (e.g. collecting facial images), and generally securing evidence (e.g. collecting DNA and fingerprints). As these aspects of police investigation practices take place within the context of a criminal process, they may have an important impact upon the fairness of a criminal trial under Article 6. These aspects include to both the presumption of innocence and evidentiary issues. Article 6 could also apply when an individual has not been formally charged in domestic law with an offence. This means that initial proceedings at the outset of a criminal process may therefore

fall within the scope of Article 6: for example, by the imposition of a requirement to give evidence. [35]

36. Article 6 (2) is particularly important in this debate as it provides that '*everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law'.* The obligation to respect the presumption of innocence not only applies to judges, but also to other public officials in general. The retention of the biometric data unconvicted persons entrenches an interim categorisation of suspicion which adheres to individuals once they have come to be charged or arrested, thus distinguishes them from 'truly' innocent people who have not come to the attention of the police.

37. The respect for due process guarantees are fundamental in relation to the right of every person under the Convention to be presumed innocent. Biometric acquisition or retention of innocent people, including those exercising the right to peaceful assembly and association may compromise the precept that everyone should be presumed innocent by the State.[36] This presumption includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal. The fact that some biometric data (e.g. DNA) is retained in the same way as the data of convicted persons is of concern in this regard.

38. Article 6 is given a purposive interpretation that furthers the principle of fairness in the administration of justice. In terms of fair rules of evidence it means the examination of the method in which the evidence was obtained[37] and admitted in the criminal proceedings.[38]

---

[35] *O'Halloran and Francis v the United Kingdom*, judgment of 29 June 2007 (ECHR).
[36] See Police facial recognition trial led to 'erroneous arrest' The controversial trial of facial recognition equipment at Notting Hill Carnival resulted in roughly 35 false matches and an 'erroneous arrest', highlighting questions about police use of the technology. Sky news 7 Sept. 2017 available at http://news.sky.com/story/police-facial-recognition-trial-led-to-erroneous-arrest-11013418
[37] *Barbera and others v Spain,* 1988 (ECHR).
[38] *Dombo BV v Netherlands*, 1993 (ECHR).

Whether evidence is of dubious quality,[39] the rights of the defence have been respected or it is improperly obtained, it is generally a matter for the national courts. However, it is important to consider that the admission of evidence that gives rise to substantive unfairness may render the criminal proceedings unfair - if other guarantees have not been respected.

39. Article 6 is also relevant when considering it together with Article 8. In assessing whether the use of evidence obtained in violation of Article 8 has render the trial unfair, the court will examine all the circumstances of the case, but in particular the respect for the defence rights and the quality and importance of the evidence in question.[40] There has been a very rapid growth of the police collecting and using facial images with differential decision making across the UK, which runs the risk of false intelligence or wrongful allegations.[41]

Article 9 to 11 - Democratic Freedoms

40. 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 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.

41. While there is a general requirement to refrain from unjustified interferences, there may be situations where law enforcement agencies

---

[39] Validation is the process of providing objective evidence that a method, process or device is fit for the specific purpose intended, i.e. can be relied upon. The Criminal Practice Directions 1 suggest that the court takes into account when determining the reliability of expert opinion, "19A.5 (a) the extent and quality of the data on which the expert's opinion is based, and the validity of the methods by which they were obtained."

[40] *Gafgen v Germany*, 2010 (ECHR).

[41] HM Inspectorate of Constabulary in Scotland: Audit and Assurance Review of Facial Search functionality within the UK Police National Database (PND) by Police Scotland, January 2016. P7.

are justified to do so. However, any interference with these rights must comply with a number of conditions if it is to be consistent with the Convention. These conditions are:

(i) the interference must be in accordance with the law;

(ii) it must be in pursuance of a legitimate aim; and

(iii) it must be necessary in a democratic society.

42. The use of biometric data, which includes the collection of facial images, iris, fingerprints and voice, 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 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 operation complies with human rights norms and international standards.

Equality and Non-Discrimination

43. 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.[42] In line with this, the Government should ensure that the principle of non-discrimination is interpreted and applied consistently by law enforcement agencies. The practice of collecting, retaining and deleting biometric data should specially consider the situation of vulnerable and disadvantaged groups, including children.

44. Public authorities[43] have a statutory duty to have due regard to: the need to eliminate unlawful discrimination, harassment, and victimisation;

[42] 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.
[43] And others carrying out public functions.

advance equality of opportunity; and to foster good relations between people who share a protected characteristic and those who do not. Fostering good relations means tackling prejudice and promoting understanding between people from different groups. This duty is often referred to as the 'equality duty' and it applies when public authorities are exercising their functions, for example when they are designing their policies and procedures and delivering services.[44] The general duty is supported by the specific duties in Scotland.

45. 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 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 be subject to close judicial scrutiny and should be periodically reviewed.[45]

46. There is a risk that certain groups are disproportionately affected by collection and retention measures in this area.[46] 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.[47] The collection and retention of biometric data of these

---

[44] See Equality Act 2010
[45] E/CN.4/2005/103, paras. 71–76
[46] 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
[47] 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.

groups may compound and increase other institutional or societal discrimination or bias.

47. 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 is not reasonably or objectively justified, are discriminatory.[48]

III. A Human Rights Approach to Biometrics

48. The Commission suggests that human rights should be mainstreamed into the strategies, policies and operational processes of policing.[49] The Commission would similarly advocate 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 the purposes of this section only three will be discussed.

Participation	Everyone has the right to participate in decisions which affect them. Participation must be active, free, and meaningful and give attention to issues of accessibility, including access to information in a form and a language which can be understood.
Accountability	Accountability requires effective monitoring of human rights standards. For accountability to be effective there must be appropriate laws, policies, administrative procedures and mechanisms of redress in order to secure human rights.

[48] See *Abdulaziz, Cabales and Balkandali v. the United Kingdom (ECHR)*
[49] See for example human rights based policing at http://www.scottishhumanrights.com/justice/policing/#policing-1244

Non-discrimination and equality	A human rights based approach means that all forms of discrimination must be prohibited, prevented and eliminated. It also requires the prioritisation of those in the most vulnerable situations who face the biggest barriers to realising their rights.
Empowerment	People should understand their rights, and be fully supported to participate in the development of policy and practices which affect their lives. People should be able to claim their rights where necessary.
Legality	The full range of legally protected human rights must be respected, protected and fulfilled. A human rights based approach requires the recognition of rights as legally enforceable entitlements, and is linked in to national and international human rights law.

49. The ***legality*** considers the explicit linkage of the proposed scheme to international, regional and domestic human rights instrument (above). A lack of current guidance and uniformly applied standard across Scotland brings serious concerns about the infringements such systems can have on the fundamental freedoms and rights of the public.

50. ***Accountability,*** which is central to the protection of human rights, requires both effective monitoring and effective remedies. Accountability to be effective requires the duty bearers to provide for the development of adequate laws, policies, institutions, administrative procedures and redress mechanisms. In this context, three aspects are crucial when debating accountability:

(1) sharing of information across state agencies

(2) outsourcing to private enterprises, and

(3) obligations to share data whether nationally or internationally under mutual assistance treaties both European and global.

51. Increased accountability will need to operate at a pan-government level as data is shared across government departments and agencies. The Council of Europe Recommendation R(92)1 ‘on the use of the

analysis of DNA within the framework of criminal justice system' sets out that samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes. Linkage and sharing of biometric data beyond criminal law purposes should be defined by law and subject to individuals' consent when appropriate. Collection of biometric data (e.g. facial images), in particular of innocent people that participate in large events also raises the issue of informed consent as highlighted above.

52. The framework should also have an effective, accessible and independent mechanism of review for the individuals concerned. For example, the biometric framework should contain a provision for independent review of the justification for the retention or refusal of destruction according to defined criteria, including such factors as the seriousness of the offence, previous arrests, utility of the retention and period, 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.[50] 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.

53. In democratic states, the protection of an open society requires also the democratic accountability and civilian control of intelligence services. The UN standards for oversight bodies clarify that is crucial to *"(E)stablish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data*."[51]

---

[50] *Segerstedt-Wiberg and Others v. Sweden,* application no. 62332/00 (ECHR)
[51] UN, GA (2016a), Resolutions on the right to privacy in the digital age, 21 November 2016, para. 5

54. 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.[52]

55. The effective ***participation*** of those affected by this policy area is crucial to ensure its legitimacy. It is equally important than some of the ethical issues are discussed widely within clearly defined purposes for public engagement and then appropriate types of engagement.

56. The acceptance by the public of the use of biometrics for crime control purposes may depend on the extent to which is discussed and the governance arrangements provided. Public debate in all aspects of collection, retention and storage of biometric data is to be encouraged. Participation must be dynamic, free and give due attention to issues of accessibility, including access to information in a form and a language which can be understood. This is paramount in a complex technical area such as biometrics.

The Commission will be pleased to further clarify any points raised in this paper.

IV. Summary

- The summary below should be read in conjunction with the full paper.
- Human rights are central to the biometric data regime, therefore the proposed framework should clearly reference human rights. The use (retention and storing) of personal data is sensitive and must be highly protected from abuse and arbitrariness.
- The Human Rights Act sets out the fundamental rights in this context. However, there is also EU law and general principles of human rights, which make clear that public authorities have a duty to adhere to, including taking full account of, and not contravene, these fundamental principles such as the respect for the human body, human dignity and the principle of proportionality in carrying out of criminal justice.
- The Commission acknowledges that the acquisition and retention of biometric information play a role in criminal justice policy and practice. However, there is a need for further interrogation around the real benefits of biometric technologies in this area. Such debate

[52] *S and Marper v UK*, para 99 (ECHR)

would ensure that any proposed regime is based on utility and public safety, which derives from sound evidence rather than anecdotal experiences.

- The use of biometrics by law enforcement agents has the potential to negatively impact on the rights of individuals and/or groups in relation to Articles 3, 5, 6, 8, 9,10, 11 and 14 of the European Convention of Human Rights. There are considerable human rights risks, therefore a robust framework should be built around those critical aspects to endure human rights and fundamental freedoms are respected.
- Any restrictions to Article 8 should be in accordance with the law, in pursuit of a legitimate aim and necessary in a democratic society. The protection afforded by Article 8 of the ECHR and HRA would be unacceptably debilitated 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 such techniques against important private life interests.
- There is a need for greater clarity about when the police and/or law enforcement agencies can collect biometric data from a person without her consent.
- Biometric data taken from individuals should be routinely deleted when it is no longer necessary to keep it for the purposes for which it was collected.
- The use of force to obtain biometric data should be avoided because it entails a high risk of violating the dignity of a person and the prohibition of inhuman or degrading treatment or punishment – this is treatment which causes severe mental or physical harm or which is grossly humiliating and undignified as to reach Article 3 of the European Convention of Human Rights
- If a person is deprived of liberty to obtain her biometric data, it is imperative for law enforcement agencies to give due consideration to the procedural and substantive guarantees articulated under Article 5 of the European Convention of Human Rights.
- Additional safeguards should be applied to the practice of collecting, retaining and storing biometric data of vulnerable and disadvantaged groups, including children. The principles of equality and non-discrimination are central to human rights law and are recognised as crucial norms in both the domestic and the international framework.
- Article 6 is important as it provides that ‘everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law’. The obligation to respect the presumption of innocence not only applies to judges, but also to other public officials in general. The retention of the biometric data unconvicted persons entrenches an interim categorisation of suspicion.
- 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.
- Private actors (e.g. business enterprises dealing with the use of biometric data) should comply with all applicable laws and respect human rights.
- Obtaining or collecting biometric data while people are exercising their democratic freedoms such as the right to freedom of peaceful assembly and association is likely to interfere with this right. Any interference with these rights must comply with a number of conditions (i) the interference must be in accordance with the law; (ii) it must be in pursuance of a legitimate aim; and (iii) it must be necessary in a democratic society.

- The Commission advocates a human rights based approach to the use of biometric data. This means that decision makers should ensure that legality, accountability, effective participation and non-discrimination are dully considered when planning, implementing and evaluating the use of biometric data.
