Independent legal review of the governance of biometric data in England and Wales

Matthew Ryder QC

The Ryder Review

Ada Lovelace Institute

June 2022

Contents

Foreword

The world is at the beginning of an ambitious new revolution in the collection, use and processing of biometric data both by public authorities and the private sector. In almost every aspect of our lives – from online identification, to health status and law enforcement – our biometric data is being collected and processed in a way that previously would have been considered unimaginable.

In order to protect our fundamental rights, particularly our data and privacy rights, this revolution in biometric data use will need to be accompanied by a similarly ambitious new legal and regulatory regime. That regime will need to be put into effect by firm, assiduous and proactive lawmakers and regulators. This is vital to ensure that we do not allow the use of biometric data across society to evolve in a flawed way, with inadequate laws and insufficient regulation.

More than 20 years ago, English law took a wrong turn in relation to the regulation of biometric data. That misstep took over a decade to rectify, and the law surrounding biometric data has struggled to stay current and effective ever since. The aim of this Review is to ensure that, at this important time, we do not take a similar wrong turn.

With hindsight, we can see how easily legal understanding of the significance of processing biometric data went awry. It is worth recalling how this happened, because of the potential parallels with the position we are in today:

In 1998 the biometric data of a man accused of burglary – his DNA sample – was retained by the police, inadvertently, and in breach of the law. After his acquittal for burglary the sample should have been destroyed. But, because it had been unlawfully retained, it was later used to identify the same man in a much more serious case. He was arrested and subsequently convicted of a horrific rape and assault that might otherwise never have been detected.

In 2001, as a direct result of that case, the law was changed not only to allow biometric data – DNA and fingerprints – to be collected in a wide range of circumstances but also to allow it to be retained almost

indefinitely. The understandable desire to provide an effective tool to those seeking to investigate crime pushed aside concerns over the consequences of collecting biometric data on a vast scale.

Within a few years the UK had created the world's largest DNA database, which included the biometric data of people who had never been charged or convicted of offences, including children. The data retained was disproportionately weighted towards those who had contact with the police, whether or not they were at fault, potentially embedding and exacerbating systemic flaws in the policing of particular communities. Young Black men, in particular, were disproportionately represented on that database.

When those raising concerns about this legal change brought legal challenges, the UK Courts, including the House of Lords, failed properly to appreciate the level of interference with rights that was caused by the accumulation of a large database. Police and courts were woefully slow to recognise how much the collection of biometric data impacted on the rights of those whose data had been retained.

It was not until a legal challenge to the DNA database in the foundational case in the European Court of Human Rights of *S and Marper v United Kingdom* [2008][1] that, very slowly, a legislative change occurred in UK law, culminating in the Protections of Freedoms Act 2012.

That legislation not only limited the scope and retention of biometric data but also created both a Biometrics Commissioner and a Surveillance Camera Commissioner in England and Wales. In 2021 those key roles were merged. In 2022 they may be changed even further by being placed within the remit of the Information Commissioner's Office, despite objection to that proposal from the current Commissioner.

Even at the time of the 2012 legislation, the law was already lagging behind technical developments. The use and range of different types of biometric data had increased dramatically from the use of fingerprints, photos and DNA contemplated by the earlier litigation. That pace of change has continued exponentially.

1 ECHR 1581; (2009) 48 EHRR 50

In the same period there was a transformation of the global economy around the use of data. Most of the world's largest companies, used by billions of people every day, are collectors and aggregators of vast amounts of personal data. Many commentators argue that weak laws and regulations on the use of personal data at the turn of the century caused our economies to become overly dependent on dysfunctional and detrimental uses of data by those major companies.[2] We should learn from those errors, and the power imbalances they perpetuate, in our regulation of biometric data in the private sector.

The desire of law enforcement, public authorities and private companies to push the legal boundaries for the use of biometric data remains. It is understandable and well intentioned. Such innovation allows them to have better information, run better services and make more efficient use of resources. But it becomes dangerous when the regulatory boundaries are unclear, and when the law fails to respond quickly and effectively to new data-processing techniques.

The increasing use of live facial recognition (LFR), which we discuss in this Review, is perhaps the clearest example of why a better legal and regulatory framework for biometric data is needed urgently. But LFR is merely the technology that has the most focus currently. The concerns it raises apply in numerous other areas. As we have set out in the Review, a new regulatory framework must be applicable to a range of biometric technologies, rather than simply react in a piecemeal way to each new development. Similarly, we strongly recommend urgent research on regulating biometric data in the context of use by private companies. We found such research to be significantly lacking, due to the particular focus thus far on biometric data use by public authorities, particularly LFR by law enforcement.

While the global COVID-19 pandemic delayed work on the Review, it also forced us to consider the use of biometric data in a context we might otherwise have overlooked. As the pandemic moves into its third year, world governments are rushing to use biometric data both for identification and categorisation, perhaps on a mandatory basis. This has profound implications and merits specific consideration

2 Most notably: Zuboff, S. (2019). *The Age of Surveillance Capitalism.* London: Profile Books.

outside the scope of the original remit of the Review. We hope our recommendations can assist in that work.[3]

It is important to acknowledge that in the last 20 years there have been huge legislative changes around the use and processing of personal data, including the EU General Data Protection Regulation (GDPR), mirrored by the UK General Data Protection Regulation. There are even more dramatic legal changes in the pipeline, such as the forthcoming EU Artificial Intelligence Draft Regulation ('the AI Act'). However, these legislative changes have not brought sufficient clarity to the regulation of biometric technologies. There remains legal uncertainty as to when, if at all, techniques such as LFR can be used in accordance with the law, and how the use of biometric data should be regulated.

This Review has sought to address that uncertainty by assessing the existing legal and regulatory framework and by making **10 recommendations**.

In arriving at those recommendations, and while taking evidence and conducting research, we were repeatedly struck by two counterintuitive features in this area.

First, strong law and regulation is sometimes characterised as hindering advancements in the practical use of biometric data. This should not be the case. In practice a clear regulatory framework enables those who work with biometric data to be confident of the ethical and legal lines within which they must operate. They are freed from the unhelpful burden of self-regulation that arises from unclear guidelines and overly flexible boundaries. This confidence liberates innovation and encourages effective working practices. Lawmakers and regulators are not always helping those who want to act responsibly by taking a light touch.

Second, the importance of transparency and public consultation was emphasised by all stakeholders, but the practical effect of such emphasis was not always positive. On the one hand, obtaining active and informed public understanding through a structured process – such as a 'citizens' jury' – could provide valuable information on which

3 See: Ada Lovelace Institute. (2021). *Checkpoints for vaccine passports*. Available at: https://www.adalovelaceinstitute.org/report/checkpoints-for-vaccine-passports/

to base policy. But too often public and private authorities were relying on the public's partially understood purported consent; an ill-defined assessment of public opinion; or the mere fact of an election victory, as a broad mandate for intrusive collection and use of the public's biometric data.

The protection of our fundamental rights in relation to biometric data is a complex area which lawmakers and regulators must not delegate to others, or allow public or private authorities to avoid merely by relying on purported public consent. Now more than ever, they have a responsibility to step up to protect the public from the harms and risks that the public themselves may not fully appreciate or even be aware of.

Lastly, I would like to thank those involved in the work of the Review.

I am grateful to my Review team: Jessica Jones, Javier Ruiz and Sam Rowe.

We would like to thank the Advisory Board who shared their time and expertise, and kept us alerted to important points as we were carrying out our work. They are, Anneke Lucasson, Lillian Edwards, Marion Oswald, Edgar Whitley, Pamela Ugwudike, Renate Samson and Matthew Rice.

We would like to express huge gratitude to all the witnesses from whom we took evidence and for their willingness to share their experiences and views. Our thanks, also, to Venetia Tate of Matrix Chambers, whose diligent organisation of the evidence sessions allowed that stage of the Review to proceed smoothly.

Most of all, I am personally grateful to those at the Ada Lovelace Institute (Carly Kind, Octavia Reeve, Imogen Parker, Madeleine Chang, George King and Sohaib Malik, in particular) who commissioned and supported this work, without ever seeking to direct it, and with considerable patience and understanding for the COVID-19-related delays that we encountered along the way.

Matthew Ryder QC
London 2022

1. Introduction

1.1 This Review was commissioned by the Ada Lovelace Institute in January 2020. Its remit was to conduct an independent, impartial and evidence-led analysis of the governance of biometric data in England and Wales, and to reach conclusions and make recommendations on regulatory reform.

1.2 The impetus for the Review was multi-faceted but a key concern, both before and after the review was commissioned, was police use of live facial recognition (LFR) technology. It received considerable public attention, following the Metropolitan Police Service's deployment of LFR[4] at Notting Hill Carnival in 2017 and South Wales Police's piloting of the same technology in 2017–18. In 2019, the Biometrics and Forensics Ethics Group noted the lack of independent oversight and governance of LFR and, in 2019 and 2020, the Divisional Court and Court of Appeal gave judgments on the lawfulness of the South Wales deployments,[5] with the Court of Appeal finding that there was an insufficient legal framework around the deployment of LFR to ensure compliance with human rights. The public and legal concerns around LFR have not diminished, but have increased substantially during the course of this Review. As recently as October 2021 the European Parliament voted overwhelmingly in favour of a resolution calling for a ban on the use of facial recognition technology in public places.[6]

4 Facial Recognition Working Group of the Biometrics and Forensics Ethics Group. (2019). *Ethical issues arising from the police use of live facial recognition technology*. Available at : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf

5 The Divisional Court judgment is available at: https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html The Court of Appeal judgment is available at: https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html

6 European Parliament. *Minutes: Wednesday 6 October 2021 – Strasbourg*. Available at: https://www.europarl.europa.eu/doceo/document/PV-9-2021-10-06-ITM-002_EN.html

1.3 The Home Office Biometrics Strategy was published in 2018, in response to the growing prominence of biometric data, but was criticised as lacking substance and for failing to set out future plans.[7] In November 2019, the Conservative Party manifesto pledged to 'empower the police to safely use new technologies like biometrics and artificial intelligence, along with the use of DNA, within a strict legal framework'.[8] But there has not yet been any new legislation, and the rapid rate of technological advance has left many concerned that existing legislative and policy frameworks are outdated and fail to account for the new and various ways in which biometric data is, or might be, accessed and used by public and private organisations alike. There has been an increasing clamour from civil liberties organisations, supported by statements from the former Biometrics Commissioner among others,[9] that human rights standards of proportionality and necessity are not being respected in the context of public-sector biometric data use. In July 2019, the Commons Science and Technology Select Committee called for 'an independent review of options for the use and retention of biometric data'[10] and, after 6 months of no response from the Government, the Ada Lovelace Institute heeded that call and established the Review.

1.4 The Review team[11] has enjoyed full independence from the Ada Lovelace Institute and has formulated its recommendations on the basis of its own analysis of the evidence received. We have benefited from the support of an expert Advisory Board (see **Annex 3**), whose expertise covers genetics, internet law, information systems, criminology and digital policy. Their input to this Review has been invaluable. So too has been the input of all the expert witnesses, who willingly shared their time and

7 Orme, D. (2018). 'Tackling the UK Government's identity crisis'. *Government & Public Sector Journal.* Available at: https://www.gpsj.co.uk/?p=4325

8 *The Conservative and Unionist Party Manifesto 2019*. Available at: https://assets-global.website-files.com/5da42e2cae7ebd3f8bde353c/5dda924905da587992a064ba_Conservative%202019%20Manifesto.pdf

9 See, for example: Biometrics Commissioner. (2019). *Annual Report 2018*, paragraph 33. Available at: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2018; Biometrics Commissioner. (2020). *Annual Report 2019*. Available at: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019

10 House of Commons Science and Technology Committee. (2019). *The work of the Biometrics Commissioner and the Forensic Science Regulator*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003.htm

11 The Review was led by Matthew Ryder QC, with a team comprising Jessica Jones, Javier Ruiz and Samuel Rowe. Short curriculum vitae of the Review team members are at **Annex 2**.

knowledge with us to shine a light on areas of predominant concern and opportunity (see **Annex 4**). We hope that this Review, representing the culmination of more than a year's work and a broad set of conversations with different interested parties, will help identify and shape the way in which a new legal framework, which rises to the challenges of biometric data use, might be established.

2. Executive summary and recommendations

2.1 Over the course of the Review, we heard several clear and consistent messages from nearly all of the individuals from whom we took evidence, irrespective of their particular interest: the current legal framework is not fit for purpose, has not kept pace with technological advances and does not make clear when and how biometrics can be used, or the processes that should be followed; the current oversight arrangements are fragmented and confusing, meaning that, for example, it is not clear to police forces to whom they should turn for advice about the lawful use of biometrics; and the current legal position does not adequately protect individual rights or confront the very substantial invasions of personal privacy that the use of biometrics can cause. There was also considerable concern about how to achieve public engagement with an area that can be technical and complex, and how to achieve a sufficient level of public understanding to ensure legitimacy and democratic accountability in the future regulation and use of biometric data.

2.2 We began the Review intending to address public and private-sector uses of biometrics in equal measure. It quickly became apparent, however, that public sector organisations were more willing to engage with the Review, more of the research which was available to us focused on public-sector uses, and the academics and civil liberties organisations we spoke to had given considerably more thought to public-sector use of biometrics than private and commercial use. That has informed the way in which this Review is, ultimately, directed predominantly at public-sector use of biometrics. Where we have felt we have a sufficiently robust evidence base to make recommendations relating to the regulation of biometrics in private sector and commercial entities, we have done so; but it is also one of our recommendations that specific, additional private-sector focused work be undertaken.

2.3 Taking account of all of this, we make the following ten recommendations:

Recommendation 1: There is an urgent need for a new, technologically neutral, statutory framework. Legislation should set out the process that must be followed, and considerations that must be taken into account, by public and private bodies before biometric technology can be deployed against members of the public.

Recommendation 2: The scope of the legislation should extend to the use of biometrics for unique identification of individuals, *and* for classification. Simply because the use of biometric data does not result in unique identification does not remove the rights-intrusive capacity of biometric systems, and the legal framework needs to provide appropriate safeguards in this area.

Recommendation 3: The statutory framework should require sector and/or technology-specific codes of practice to be published. Such codes should set out specific and detailed duties that arise in particular types of cases.

Recommendation 4: A legally binding code of practice governing the use of LFR should be published as soon as possible. We consider that a specific code of practice for police use of LFR is necessary, but a code of practice that regulates other uses of LFR, including use by private entities and public-private data sharing in the deployment of facial recognition products, is also required urgently.

Recommendation 5: The use of LFR in public should be suspended until the framework envisaged by Recommendations 1 and 4 is in place.

Recommendation 6: The framework envisaged by Recommendations 1 and 4 should supplement, and not replace, the existing duties arising under the Human Rights Act 1998, Equality Act 2010 and Data Protection Act 2018.

Recommendation 7: A national Biometrics Ethics Board should be established, building on the good practice of the London Policing Ethics Panel and West Midlands Police, and drawing on the expertise and experience of the Biometrics and Forensics Ethics Group. This Board should have a statutory advisory role in respect of public-sector biometrics use.

Recommendation 8: The Biometrics Ethics Board's advice should be published. Where a decision is taken to deploy biometric technology contrary to the advice of the Biometrics Ethics Board, the deploying public authority should publish a summary explanation of their reasons for rejecting the Board's advice, or the steps they have taken to respond to the Board's advice. The public authority's response should be published within 14 days of the decision to act contrary to the Biometrics Ethics Board's advice and prior to deployment.

Recommendation 9: The regulation and oversight of biometrics should be consolidated, clarified and properly resourced. The overlapping and fragmented nature of oversight at present impedes good governance. We have significant concerns about the proposed incorporation of the role of Biometrics and Surveillance Camera Commissioner into the existing duties of the ICO. We believe that the prominence and importance of biometrics means that it requires either a specific independent role, and/or a specialist Commissioner or Deputy Commissioner within the ICO. Wherever it is located, it must be adequately resourced financially, logistically, and in expertise, to perform the governance role that this field requires.

Recommendation 10: Further work is necessary on the topic of private-sector use of biometrics. While we consider that the statutory framework envisaged by Recommendation 1 *must* regulate private-sector use to some extent, many of those we interviewed had extensive knowledge about public-sector use of biometrics but much less experience and expertise in the challenges and issues arising in the private sector. There are plainly considerable, rights-engaging concerns around private-sector use of biometrics, but we have not received enough private-sector input to the Review to be able to propose detailed solutions. We recommend that further, private-sector-specific research and evidence gathering is undertaken. This is particularly important given the porous relationship between private-sector organisations gathering and processing biometric data and developing biometric tools, and public authorities accessing those datasets and deploying those tools.

3. Our methodology

3.1 The work of the Review involved three core strands: (1) research undertaken by the Review team; (2) interviews with various interested parties; and (3) liaison with the Advisory Board.

Research

3.2 The recent prominence of biometrics as a topic of public interest and debate has resulted in the publication of numerous reports and papers which we considered carefully. These include work from leading UK organisations such as the Centre for Data Ethics and Innovation, the Royal United Services Institute, the Alan Turing Institute and the Biometrics and Forensics Ethics Group, among others. In addition to these reports, the Review team also considered the relevant statutory reports from regulators and public bodies such as the Biometrics and Surveillance Camera Commissioners.

3.3 Our policy research was not limited to the UK. It included analysis of international developments, mainly in the US and EU. Our sources were varied,[12] ranging from reputable media outlets covering the extensive developments in those countries to policy publications from think tanks – prominently the AI Now Institute – along with organisations such as the American Civil Liberties Union and public bodies such as the National Institute of Standards and Technology (NIST), which is a global authoritative reference for the technical accuracy of certain biometrics. EU organisations, from the European Data Protection Board to various units in the European Commission and Parliament, have been active in the development of the conceptual underpinning on biometrics and regulatory initiatives.

12 It is appropriate here to acknowledge the helpful and extensive news developments on biometric data that can be found at https://www.biometricupdate.com.

3.4 Besides policy, advocacy and legal documents, we also reviewed academic literature in the fields of social sciences and humanities, where there is a helpful body of work on the study of the social impacts of algorithms and data, often in interdisciplinary approaches with legal scholars and computer scientists. These newer developments on social impact complement the existing analyses from areas such as surveillance studies or science and technology studies.

3.5 We also surveyed the technical literature on biometrics to the best of our abilities. Although our team did not include computer scientists or biometric technologists, several members have experience in the analysis of technical systems and were supported by the Advisory Board in this regard. This approach ensured that the Review's recommendations and analysis have been informed by the science. The literature on facial recognition and algorithms is particularly extensive and includes both academic journals and a variety of online publications, some of it from technology companies such as Facebook and Google but also from independent researchers and developers, showing the very dynamic nature of this area. Other areas where scientific literature provides necessary insights are the role of training datasets, accuracy, bias and new biometric modalities.

Interviews

3.6 We took evidence from 24 individuals over a series of interviews conducted between September 2020 and February 2021. Some of our interviews were with a single individual, while some took place in a small group. Each interview lasted between an hour and an hour-and-a-half and addressed a series of themes identified by the Review team as being of particular interest, though with sufficient flexibility to respond to the particular interests and expertise of those with whom we talked. Our interview timetable was delayed by the COVID-19 pandemic and lockdown arrangements that were introduced. Nevertheless, once arrangements had been put in place for the taking of evidence remotely, we were able to obtain a comprehensive cross-section of evidence from individuals engaged with biometrics and their use in the public sector, which has underpinned and provided the basis for the recommendations put forward in this Review. We spoke to, among others, the then

Biometrics Commissioner, the then Forensic Science Regulator, the then Surveillance Camera Commissioner, Home Office ministers, the Information Commissioner's Office, the Metropolitan Police Service, West Midlands Police, the College of Policing, the Centre for Data Ethics and Innovation, AI Now, Liberty and Big Brother Watch. A full list of the interviewees who agreed to be on the record is at **Annex 4**. We were also assisted by several off-the-record conversations which provided useful background. The Review team received less engagement from private-sector organisations, and the more limited scope of the evidence that was received on the issues arising from private sector and commercial use of biometrics is reflected in the recommendations that the Review puts forward, in particular Recommendation 10 which recognises that there is further work to be done on this aspect.

Advisory Board

3.7 The Review team were also assisted by several meetings with the Advisory Board, who provided useful direction, resources and contacts, and who asked thought-provoking questions, which helped to steer the focus of the Review.

4. What is biometric data?

4.1 Most members of the public have a general understanding of biometric data – that it is personal data, often obtained from or relating to a person's body or behaviour, which may be used to uniquely identify them. Thus, the most common forms of biometrics in use, and recognised by the public, are a person's fingerprints and DNA. Iris scans, voice recognition and facial recognition are also forms of biometrics that are part of the public consciousness. Less well-known are the more novel forms of biometrics such as behavioural traits like gait analysis or key-stroke analysis. As technology advances, so too will the forms of biometric data which can be derived from individuals. Indeed, data relating to physical and physiological characteristics of an individual have fallen within the definition of biometric data for several years,[13] but data relating to behavioural characteristics are novel, having been aided by developments in big data analysis. In his evidence to the Review, the former Biometrics Commissioner considered that the addition of behavioural data 'significantly broadens what had previously been thought about as biometrics'.[14]

4.2 One of our first tasks was to consider the current scope of what constitutes biometric data, in order to determine the focus of the Review. Various organisations and legal instruments provide different definitions of biometric data, and we considered those alternatives and the potential repercussions of choosing one over another, in terms of the safeguards that would apply to privacy-invading practices or systems. We also discussed the difficulty of defining biometrics with those who gave evidence to the Review, discovering that there were differences of opinion as to the importance of the definition and which definition should prevail.

4.3 When considering biometric data, there are two relevant stages: first, identifying what it is; and secondly, identifying what requirements must be met when processing it. At the first stage,

13 Explanatory Notes to the Protection of Freedoms Act 2012.
14 Biometrics Commissioner, interviewed 9 November 2020.

the focus is on the inherent properties of the data. At the second stage, the focus shifts to consider why the data is being processed. Both stages are, in our view, relevant to the safeguards that should attach to biometric data.

4.4 Our foundational starting point was the UK General Data Protection Regulation (UK GDPR) which, consistent with the EU GDPR and the Law Enforcement Directive,[15] defines biometric data 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 data'.[16] That definition is made up of three elements. First, the data's source; secondly, how the data was obtained; and finally, the data's ability to identify an individual uniquely. The ICO believes that the second stage is the operative part of the definition, stating that 'it is the type of processing that matters'.[17]

4.5 Although the GDPR definition was our starting point, we looked closely at other definitions employed by different organisations. For example, the Article 29 Working Party in its Opinion on the Concept of Personal Data offered an alternative description which focuses on two components (and not on how the data was obtained): for them, biometric data is 'biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability'.[18]

4.6 Common to both the UK GDPR and Article 29 Working Party definitions is a requirement that the data at least has the capacity to uniquely identify a person. The capacity for unique identification was considered to be important by a number of interviewees,

15 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. Available at: http://data.europa.eu/eli/dir/2016/680/oj

16 Data Protection Act 2018, Section 205(1); GDPR, Article 4(14).

17 Information Commissioner's Office (ICO). (2021). *Information Commissioner's Opinion: The Use of Live Facial Recognition Technology in Public Places*, Section 4.1. Available at: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

18 Article 29 Data Protection Working Party, *Opinion 4/2007* (WP136, 2007), p. 8.

as well.[19] There is, however, some debate regarding the extent of individuation that is necessary before information is considered to be biometric data. During her interview, the then Forensic Science Regulator expressed some concern that 'there is no such thing as absolute identification from biometrics',[20] which would undermine the usefulness of a definition that required absolute unique identification in order for safeguards to be engaged. The courts have dealt with the probabilistic nature of biometric data pragmatically. In *R (Bridges) v Chief Constable of South Wales Police* ('*Bridges*'), a case about police use of automatic live facial recognition technology on crowds, the High Court (in a definition also adopted by the Court of Appeal) stated that 'biometric data enables the unique identification of individuals with some accuracy. It is this which distinguishes it from many other forms of data.'[21] Consequently, there should be no expectation that the biometric data will be capable of identifying an individual with total accuracy, but it should at least be capable of providing a confident identification.

4.7 We agree that the capacity to uniquely identify individuals with some, but not absolute, certainty is a central feature of biometric data, as it is a feature of all personal data. But that does not mean, we think, that only data being processed *for the purposes* of unique identification (the second stage identified at 4.3 above) should fall within a framework for the regulation of biometrics.

4.8 We concluded that, where data which has the capacity to uniquely identify individuals with some confidence is obtained or used for purposes other than unique identification – for example, where facial images are captured which could identify individuals but which are used instead for classifying them into race or sex categories – that use, or systems that provide for such activity, must also be subject to robust, rights-safeguarding regulation equivalent to the regulation necessary where identification actually takes place.

19 Amba Kak, interviewed 8 October 2020; Centre for Data Ethics and Innovation, interviewed 9 December 2020.

20 Forensic Science Regulator, interviewed 11 November 2020.

21 *R (Bridges) v Chief Constable of South Wales Police and Secretary of State for the Home Department* [2019] EWHC 2341 (Admin), paragraph 42.

4.9 We note that this is not currently the case under UK GDPR, which only introduces 'special category' protections in respect of biometric data where the purpose of the processing is for unique identification.

4.10 In our view, however, the fact of unique identification is not necessarily more rights-intrusive than the use of sensitive personal data, from which identification could be obtained, for classification or other purposes. Both scenarios require appropriate and careful regulation. Our conclusion is consistent with the views of the Information Commissioner's Office, the European Commission, the European Data Protection Supervisor and the European Data Protection Board. We have approached our recommendations (and in particular, Recommendation 2) on this basis.

5. The existing legal framework for the governance of biometric data in England and Wales

5.1 The governance of biometric data at present relies on a patchwork of overlapping laws addressing data protection, human rights, discrimination and criminal justice issues. There is no single overarching legal framework for the management of biometric data. Sources of law that developed in response to more general issues cater for the management and regulation of biometric data in an ad hoc manner.

Human rights law

5.2 Human rights law regulates the treatment of individuals by public authorities. The primary relevant legal instrument is the Human Rights Act 1998 (HRA), which implements as part of UK domestic law many of the rights protected by the European Convention on Human Rights (ECHR).

5.3 The HRA is relevant to the regulation of biometric data because it protects the right to privacy. By Section 1 of the HRA, key provisions of the ECHR form part of the law of England and Wales, including Article 8 which protects the right to privacy.

5.4 Section 6 of the HRA makes it unlawful for public authorities to act incompatibly with the rights protected by Section 1 of the HRA. Public authorities are therefore under a duty to respect an individual's right to privacy as enshrined by Article 8. It is important to note that the HRA only places duties on public authorities – private companies do not, generally, owe human rights obligations towards individuals, and this is a potential lacuna in the regulation of biometric data use by entities other

than public bodies.[22]

The concept of private life and its application to biometrics

5.5 The concept of 'private life' within the meaning of Article 8 includes the collection and retention of biometric data about a person. In *S and Marper v United Kingdom* [2008] ECHR 1581 ('*S and Marper*'), a case about the collection and retention of fingerprint and DNA data, the Grand Chamber of the European Court of Human Rights held that, '[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention'. The collection of biometric data about a person 'allowing his or her identification with precision in a wide range of circumstances' is, in the Court's view, 'capable of affecting his or her private life' and gives rise 'to important private-life concerns'. Indeed, in *Aycaguer v France* [2017] ECHR 587, a case about DNA retention, the Court went as far as to say that 'personal data protection plays a primordial role in the exercise of a person's right to respect for his private life enshrined in Article 8 of the Convention.'

5.6 In *Gaughran v Chief Constable of Northern Ireland* [2015] UKSC 29, the Supreme Court endorsed the position that 'the indefinite retention of a person's DNA profile, fingerprints and photograph interferes with the right to respect for private life recognised by Article 8(1).' In *Bridges*, the High Court held that Article 8 is engaged 'if biometric data is captured, stored and processed, even momentarily'. In this regard, 'the fact that the process involves the near instantaneous processing and discarding of a person's biometric data...does not matter'; the Court of Appeal agreed.

5.7 Interference with a person's private life may be justified if it is 'in accordance with law' and 'necessary in a democratic society' for the purposes of a legitimate aim.

22 Partly to avoid this kind of gap, domestic courts may themselves develop private law rights to ensure consistency with the protection of human rights – through the principle of 'horizontal effect'.

5.8 In *S and Marper*, the European Court of Human Rights noted that, for the collection and retention of biometric data to be 'in accordance with law', it is essential 'to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, among other things, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness'. In *R (Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9, at paragraph 11, Lord Sumption JSC described the purpose of the 'in accordance with law' requirement as follows:

'Its purpose is not limited to requiring an ascertainable legal basis for the interference as a matter of domestic law. It also ensures that the law is not so wide or indefinite as to permit interference with the right on an arbitrary or abusive basis.'

5.9 In *Bridges*, the Court of Appeal held that South Wales Police's piloting of LFR had not satisfied the 'in accordance with law' requirement and, accordingly, violated Article 8.

5.10 If a measure is in accordance with law, the next step in justifying its interference with Article 8 is to consider whether it is 'necessary in a democratic society'. That requires identifying a relevant legitimate aim and assessing whether the interference is a proportionate means of pursuing that legitimate aim. Proportionality is assessed by reference to a four-stage test (set out by the Supreme Court in e.g. *Bank Mellat v HM Treasury (No 2)* [2013] UKSC 39:

1. Whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right.

2. Whether it is rationally connected to the legitimate aim.

3. Whether a less intrusive measure could have been adopted without unacceptably compromising the objective.

4. Whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.

5.11 All of these criteria will need to be satisfied in order for the collection and retention of biometric data to be compatible with the requirements of the HRA.

Data protection law

5.12 The legal framework on the protection of personal data consists of (1) the UK General Data Protection Regulation (UK GDPR), and (2) the Data Protection Act 2018 (DPA 2018). These are relevant to biometric data because biometric data is, essentially, a sub-category of personal data.

5.13 UK GDPR and DPA 2018 define biometric data as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data' (UK GDPR, Article 4(14); DPA 2018, Section 205). Personal data is defined as 'any information relating to an identified or identifiable natural person ("data subject")' (UK GDPR, Article 4(1); DPA 2018, Section 3(2)). 'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (UK GDPR, Article 4(1); DPA 2018, Section 3(3)).

5.14 Data protection law governs the lawful processing of personal data. In this context, 'processing' means any operation or set of operations performed on personal data or sets of personal data, including collection, recording, storage, retrieval, consultation, use and disclosure, among others (UK GDPR Article 4(2), DPA 2018, Section 3(4)). Processing must demonstrate compliance with the Data Protection Principles set out in Article 5 of UK GDPR, which stipulates that personal data shall be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy', which includes a right of rectification of inaccuracies)

5. 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 ('storage limitation')

6. 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 ('integrity and confidentiality').

5.15 Part 2 of the DPA 2018 addresses the general processing of data and provides for the same rights for the data subject as arise under UK GDPR – for example, the right of access to data, the right of rectification where data is incorrect, and the right of erasure. Section 10 of the DPA 2018 makes provision for the processing of 'special category data' (defined by Article 9 of UK GDPR), which includes biometric data if the purpose of processing is to uniquely identify an individual.[23] It should be noted that there is an ongoing debate regarding what is meant by 'the purpose of uniquely identifying an individual'.[24] This Review considers that the phrase refers to the purpose of processing under the UK GDPR, Article 5(1)(b) (the 'purpose limitation' principle), since doing so

23 The phrase 'for purposes of uniquely identifying' was added during the GDPR trilogue in 2016, although no official record of that trilogue, or the rational for adopting the phrase, exists. See Council position, 05419/1/2016, April 8, 2016. The words were added later during the trilogue in 2016.

24 See: Clifford, D. (2019). *The Legal Limits to the Monetisation of Online Emotions*, pp. 177–183. Available at: https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS2807964&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US

follows the words' natural and ordinary meaning. Even where 'purpose of uniquely identifying' is construed broadly, for example encompassing any instance that a biometric template is generated for an individual to achieve comparison with others,[25] it will still fail to capture all methods of biometric classification.

5.16 UK GDPR prohibits the processing of special category data other than in certain limited circumstances, similar to those permitted under the DPA 2018. The DPA 2018 allows for the processing of special category data for the purposes of employment, social security and social protection, health and social care, public health, archiving, research and statistics, in relation to criminal convictions or offences, or where there is a substantial public interest, if the relevant conditions in Schedule 1 of the DPA 2018 are met. Part 2 of the DPA 2018 applies to both public and private sector organisations and individuals.

5.17 The operative definition of special category data means that biometric data only qualifies as special category data if it is used for the purpose of uniquely identifying an individual. This means that there will be circumstances where biometric data is used to profile individuals or groups. This data will *not* be required to meet the higher bar imposed on the processing of special category data, unless it falls under one of the other existing forms of special category data, such as data revealing racial origin. That means fewer safeguards exist where, for example, biometric analysis is used to profile individuals for job worthiness[26] but without uniquely identifying anyone. Such practices could have effects on an individual that are just as serious as those arising from unique identification. We consider that position to be unsatisfactory. As addressed above, in section 4 of this Review, the use of biometrics for classification has the potential to be just as rights-intrusive as their use for unique identification and, in our view, similar safeguards should apply.

25 *Bridges* at paragraph 133.

26 Electronic Privacy Information Centre. (2019). *In re HireVue*. Available at: https://epic.org/privacy/ftc/hirevue/

Data protection in the context of law enforcement

5.18 Part 3 of the DPA 2018 provides for the processing of personal data by competent authorities for criminal law enforcement purposes.[27] Pursuant to Section 30 and Schedule 7 of the DPA 2018, 'competent authorities' for the purposes of Part 3 includes police, prosecuting authorities, and 'any United Kingdom government department other than a non-ministerial government department', but not the intelligence services (the processing of personal data by the intelligence services is covered by Part 4 of the DPA 2018).

5.19 Section 31 of the DPA 2018 defines 'law enforcement purposes' as 'the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. By Sections 35–40, similar general data protection principles to those contained in UK GDPR apply in the context of processing for law enforcement purposes. Provision is also made for 'sensitive processing', which includes the processing of biometric data, for the purpose of uniquely identifying an individual (Section 35(8)(b)). Pursuant to Section 35, 'sensitive processing' of personal data is only lawful if consent has been obtained from the data subject or the processing, or it is 'strictly necessary', and if it meets at least one of the conditions in Schedule 8 of the DPA 2018 (i.e. it is (a) necessary 'for the exercise of a function conferred on a person by an enactment or rule of law' or (b) necessary 'for reasons of substantial public interest' or (c) necessary 'for the administration of justice'). Whether the data controller is relying on consent or strict necessity, they must have an appropriate policy document in place at the time the processing is carried out.

5.20 The test of necessity 'is a strict one, requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest. The exercise therefore involves a classic proportionality analysis'.[28] The assessment also requires 'direct personal evaluation', not a generalised evaluation.[29] ICO guidance

27 Part 3 was intended to transpose into domestic law the EU Data Protection Directive 2016/680 (Law Enforcement Directive).

28 *Guriev and others v Community Safety Development (UK) Limited* [2016] EWHC 643 (QB), at paragraph 45.

29 *R (El Gizouli) v. Secretary of State for the Home Department* [2020] 2 UKSC 10, at paragraph 44.

suggests that 'strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through some less intrusive means.'[30]

5.21 In *Zaw Lin v Commissioner of the Police of the Metropolis*,[31] the High Court noted that the 'raison d'être' of the Data Protection Act 1998 (the precursor statute to the DPA 2018) was to act as 'a protector of an individual's fundamental rights'.[32] As a consequence, 'when construing the DPA...decision makers and courts must have regard to all relevant fundamental rights that arise when balancing the interest of the State and those of the individual. There are no artificial limits to be placed on the exercise.'[33] Thus, the data protection and human rights statutory frameworks are not independent of each other, but overlap and inform the interpretation of lawful action overall.

Data protection in the context of intelligence services

5.22 Part 4 of the DPA 2018 addresses intelligence services processing. Section 82(2) describes the 'intelligence services' as the Security Service (MI5), the Secret Intelligence Service (MI6) and GCHQ. The structure of Part 4 mirrors that of Part 3 (law enforcement processing), although its content is more akin to Part 2 (general processing). Under Section 86(7)(c), biometric data processed for the purpose of identifying someone uniquely is categorised as 'sensitive processing'. Processing sensitive data is only permitted if one of the conditions in Schedule 9 is met, as well as one of the additional conditions in Schedule 10.[34]

Criminal justice and terrorism legislation

5.23 Police and other law enforcement authorities have specific powers for the collection and retention of biometric data through a range of

30 ICO. *Guidance to Law Enforcement Processing: Conditions for sensitive processing*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/conditions-for-sensitive-processing/

31 [2015] EWHC 2484 (QB).

32 At paragraph 80.

33 At paragraph 69.

34 See: Section 86(2)(b).

criminal justice and anti-terrorism legislation. The most commonly invoked powers are those contained in the Police and Criminal Evidence Act 1984 (PACE), as amended by the Protection of Freedoms Act 2012 (PoFA).

Police and Criminal Evidence Act 1984

5.24 Sections 61 – 64A of PACE give the police the power to take fingerprints, 'intimate samples', 'non-intimate samples' and photographs of suspects subject to criminal investigation. Section 65 of PACE defines intimate and non-intimate samples. Both either amount to biometric data themselves, or are sources from which the biometric data of subjects could be extracted.

5.25 PACE also contains provisions requiring the deletion of biometric data. For example, Section 63D of PACE requires fingerprints and DNA profiles derived from DNA samples ('Section 63D material') to be destroyed if it appears they were taken unlawfully or on the basis of an unlawful arrest or an arrest premised on mistaken identity. In any other case, Section 63D material must be destroyed unless it is retained under a power contained in Sections 63E – 63O of PACE. For example, Section 63E of PACE allows for the retention of Section 63D material until the conclusion of the investigation into the offence, or the conclusion of the proceedings if the investigation gives rise to proceedings. Section 63F allows for the retention of Section 63D material obtained from a person charged with, but not convicted of, a qualifying offence for three years from the date the biometrics were obtained – extendable to a period of five years on application to a District Judge. Where a person was convicted of a qualifying offence (as defined in Section 65A of PACE), by Section 63I of PACE, the police have the power to retain their Section 63D material indefinitely.

5.26 Section 63R of PACE requires all DNA samples taken from individuals to be destroyed as soon as a DNA profile has been obtained from them (though this obligation is subject to the provisions on retention of criminal evidence contained in the Criminal Procedure and Investigations Act 1996 which provides for the retention of evidence if it may be required for disclosure to the defence).

Terrorism Act 2000

5.27 Pursuant to Schedule 7 and 8 of the Terrorism Act 2000 (TACT 2000), police have the power to stop, question and detain for up to 6 hours any persons at ports or border areas for the purposes of determining whether they appear to be a person who has been concerned in the commission, preparation or instigation of acts of terrorism; and, when conducting a stop under Schedule 7, pursuant to paragraph 2 of Schedule 8, an authorised person (which includes a police officer, prison officer, or person otherwise authorised by the Secretary of State) may 'take any steps which are reasonably necessary for – (a) photographing the detained person, (b) measuring him, or (c) identifying him'. Paragraph 10 of Schedule 8 sets out when fingerprints and non-intimate samples may be taken, including being taken without consent when authorised by a superintendent under paragraph 10(4), 10(6) and 10(6A).

5.28 Paragraphs 20A–20E of Schedule 8 make provision for the destruction and retention of samples obtained during Schedule 7 stops, with the general requirement being that they are retained for no more than 6 months unless a national security determination is made that authorises their retention for a longer period.

5.29 Other similar provisions for the retention of biometric data in an anti-terrorist context appear in the Counter-Terrorism Act 2008 and the Terrorism Prevention and Investigation Measures Act 2011. The Counter-Terrorism and Border Security Act 2019, which is currently only partially in force, also contains provisions (in Schedule 3) enabling the taking of samples and fingerprints from individuals detained for questioning at a port or border area.

5.30 In the national security and criminal justice context, it is worth noting the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) which provide a coercive power to require an individual to provide a 'key' or password for the accessing of electronic information obtained with appropriate authorisations (see e.g. Section 49 of RIPA). While not explicitly relating to biometric data, Section 56(1), defines 'key' as 'any key, code, password, algorithm or other data the use of which (with or without other keys) (a) allows access to the electronic data, or (b) facilitates the putting of the data into an intelligible form'. Whether this would now be interpreted to include requiring an individual to provide

biometric data to access a device remains an open and untested legal question.

Investigatory Powers Act 2016

5.31 The Investigatory Powers Act 2016 (IPA) does not set out specific provisions relating to biometric data. However, under Part 7, it regulates the intelligence services' powers to retain 'bulk personal datasets' of personal data, which would include biometric data. Section 206 specifically contemplates such powers being used for health records.

Protection of Freedoms Act 2012

5.32 The Protection of Freedoms Act 2012 (PoFA) deliberately includes provisions to regulate the processing of biometric data – in particular, DNA, fingerprints, photographic images and video surveillance. It was enacted partly in response to the European Court of Human Rights' decision in *S and Marper* that found the UK in violation of the Article 8 rights of those whose data was retained on a DNA database.

5.33 Sections 1–19 of PoFA inserted the various provisions for the retention and deletion of biometric data discussed above (see 5.24) into PACE. Alongside those provisions, Section 20 of PoFA provides for the appointment and functions of the Biometrics Commissioner (see 5.50, below), whose responsibility it is to make national security determinations for the retention of biometric data and keep under review the use and retention of biometrics pursuant to the statutory powers in PACE, TACT 2000, the Counter-Terrorism Act 2008 and the Terrorism Prevention and Investigation Measures Act 2011. Section 21 of PoFA also obliges the Commissioner to report annually on the carrying out of their functions. Separately, Section 34 of PoFA establishes the role of Surveillance Camera Commissioner (see 5.52, below).

5.34 Chapter 2 of Part 1 of PoFA makes provision for the protection of biometric information of children in schools. Section 26 requires that parents are informed of an intention by a school to process a child's biometric information, and prohibits such processing unless

at least one parent consents to the information being processed. Even if a parent consents, by Section 26(5), if the child refuses to participate or continue to participate in anything that involves the processing of the child's biometric information, or otherwise objects to the processing of the information, the processing may not continue irrespective of the parent's consent. In such circumstances, the school 'must ensure that reasonable alternative means are available by which the child may do, or be subject to, anything which the child would have been able to do, or be subject to, had the child's biometric information been processed' (Section 26(7)).

Equality and anti-discrimination legislation

5.35 The Equality Act 2010 contains a number of provisions that bear on the use of biometric data. First, the Equality Act prohibits direct and indirect discrimination on the basis of any of a list of specified 'protected characteristics': age, disability, gender reassignment, marriage or civil partnership, race, religion or belief, sex and sexual orientation.

5.36 The prohibition of indirect discrimination means that even a policy or practice which is ostensibly neutral will be unlawful if it produces a disproportionate disadvantageous effect on people with a protected characteristic. Accordingly, systems for the collection, processing and storing of biometric data will need to comply with the requirement not to indirectly discriminate against people with protected characteristics (for example, they must not disproportionately impact people of a certain race or certain sex) in order to be compatible with the Equality Act 2010. This is particularly significant in relation to existing law enforcement tools that rely on biometric data, that are alleged to have significant differences in their reliability rates between men and women, or between people of different ethnicities.

5.37 Alongside the prohibition of substantive discrimination, the Equality Act 2010 also imposes a procedural 'public sector equality duty', or 'PSED', with which public authorities must comply whenever they make decisions in the exercise of their functions. The duty is to have 'due regard' to the impact of decisions on the statutory equality aims, namely, the need to:

1. Eliminate discrimination, harassment, victimisation and any other conduct prohibited under the Equality Act.

2. Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.

3. Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

5.38 The PSED is a process duty, rather than an obligation to achieve a particular result. It will be discharged if a decision-maker can show they have had due regard to (i.e. taken appropriate account of) the statutory equality aims, whether or not their decision actually achieves those aims. That does not, however, diminish its importance. The Court of Appeal observed in *Bridges*, that compliance with the PSED 'helps to reassure members of the public, whatever their race or sex, that their interests have been properly taken into account before policies are formulated or brought into effect'.

5.39 The PSED also requires a public authority to obtain the information necessary to properly assess the impact of their decision on the statutory equality aims – so that, for example, when technology is deployed, the public authority seeking to use it must satisfy itself that it does not have any inbuilt bias, or any bias that does exist can be overcome. As Megan Goulding from Liberty observed when giving evidence to the Review, the PSED 'might mean that companies are forced to give more information to public authorities regarding training datasets so that an investigation into bias can be done before biometric technologies are deployed'.

5.40 The possibility identified by Megan Goulding arises, in part, because the PSED is a 'non-delegable duty' which falls on a public decision-maker personally.[35] Other than in expressly permitted circumstances, it is not possible for a public authority to 'outsource' or forego its obligation to consider statutory equality objectives which arise under the PSED, on the basis that they have

35 See: *R (Brown) v Secretary of State for Work and Pensions* [2009] EWHC 3158 (Admin) at [94]; but also: *Panayiotou v London Borough of Waltham Forest* [2017] EWCA Civ 1624 at [79].

purportedly been considered at some earlier stage by another party. This is of critical importance in the context of the use of technology products that rely on the processing of biometric data: as was made clear in *Bridges*, it is not enough that a commercial provider of relevant software tells a public authority that there are no adverse equality impacts – the public authority must be in a position to give 'due regard' itself to that question.

5.41 However, what will constitute 'due regard' for the purposes of discharging the PSED is a fact-sensitive question. It is not possible to say categorically what a decision-maker will be required to do in any particular case. We do not consider that it will generally require the relevant decision-maker to have the technical expertise to understand the operation of any relevant software, but we do consider that they will require sufficient information (whether by way of summaries, explanation or statistics) about the practical operation of the software to have an understanding of the way in which its operation interacts with the statutory equality objectives. That may include, for example, a need to have some information about the datasets on which an algorithm was trained in order to identify any adverse equality effects it might be expected to cause.

Regulation and oversight

The Information Commissioner's Office

5.42 The ICO is the primary oversight body with a remit which includes biometrics. The ICO is an independent public body acting as the supervisory authority for data protection and freedom of information; and biometrics therefore falls within its scope by virtue of its status as a form of personal data.

5.43 The ICO's general powers are described in Schedule 13 to the Data Protection Act 2018 (DPA 2018). They are split across the issuance of information, assessment and enforcement notices. Its powers are regulated by safeguards (see DPA 2018 Sections 115(5) to 115(9)). Pursuant to powers under Part 6 of the DPA 2018, the ICO can take various enforcement measures against individuals and organisations who breach data protection law. These include the imposition of pecuniary penalties and prosecution, with the consent of the Director of Public Prosecutions, for criminal

offences (including, for example, unlawfully obtaining personal data).

5.44 The ICO has a duty to advise Parliament and the Government on administrative measures concerning individuals' rights and freedoms in relation to the processing of personal data (DPA 2018, Section 115). It has published codes of practice (under the Data Protection Act 1998, but which remain relevant under the DPA 2018 regime) which have a bearing on the processing of biometric data, for example: (i) the Anonymisation code of practice;[36] (ii) the CCTV Code of Practice;[37] (iii) the Employment Practices Code;[38] and (iv) the Employment Practices Code: Supplementary Guidance.[39]

5.45 It has a statutory obligation to produce at least four codes of practice under the DPA 2018 (Sections 121 – 124). Two statutory codes of practice have been issued so far: the Data Sharing Code[40] and the Age Appropriate Design Code.[41] Both give very little specific guidance relating to the processing of biometric data. Further statutory codes of practice may be issued in due course by the Secretary of State pursuant to Section 128 of the DPA 2018.

5.46 Under Section 116(2) of the DPA 2018, in conjunction with Schedule 13(2)(d), the Information Commissioner may issue formal Opinions to Government, other institutions or bodies as well as the public, on any issue related to the protection of personal data. This may form the basis for the Information Commissioner's approach to enforcement.

5.47 Two relevant examples of this role of the ICO are its two Opinions on facial recognition technology.

---

36 ICO. *Anonymisation: code of practice*. Available at: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

37 Note: this code is no longer available on the ICO's website.

38 ICO. The employment practices code. Available at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

39 ICO. *The Employment Practices Code: supplementary guidance*. Available at: https://ico.org.uk/media/for-organisations/documents/1066/employment_practice_code_supplementary_guidance.pdf

40 ICO. *Data sharing: a code of practice*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

41 ICO. *Age Appropriate Design Code*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/

5.48 The first was *The use of live facial recognition technology by law enforcement in public places,* published in October 2019.[42] Although it was published before the Court of Appeal decision in *Bridges* it was a prescient document, correctly anticipating the direction the law would take and reflecting the position the ICO took as an intervener in the *Bridges* litigation. Nine 'key messages' are summarised in the opinion including the following:[43]

'The Commissioner intends to work with relevant authorities with a view to strengthening the legal framework by means of a statutory and binding code of practice issued by government. In the Commissioner's view, such a code would build on the standards established in the Surveillance Camera Code and sit alongside data protection legislation, but with a clear and specific focus on law enforcement use of LFR and biometric technology. It should be developed to ensure that it can be applicable to current and future biometric technology.'

5.49 The second was *The use of live facial recognition technology in public places*, published in June 2021[44], which considered the use of similar technology but not in the law enforcement context covered by the earlier opinion. It examines biometric technology use both for identification and for categorisations of persons. A key issue raised, but not entirely resolved, in that opinion is who should bear the responsibility for the use of badly designed biometric technology, and what burden is there on the user of that technology to make detailed enquiry of the vendor/manufacturer. This reveals how the ICO's Opinions, while welcome, are not able to conclusively resolve some of the more difficult legal issues. But it can highlight areas that will require better guidance, new legal provisions, or – ultimately – judicial determination.

42 ICO. (2019). *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places.* Available at: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

43 ICO. (2019). p.3.

44 ICO. (2021). Information Commissioners' Opinion:The use of live facial recognition technology in public places. Available at: https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

The Biometrics and Surveillance Camera Commissioner(s)

5.50 The Biometrics Commissioner was established under Section 20 of the Protection of Freedoms Act 2012 (PoFA). The Biometrics Commissioner is independent of Government. Despite the generality of the role's title, the Commissioner does not have a general remit over all public issues relating to the use of biometrics, but has four specific statutory functions:

1. Reviewing the retention and use of DNA samples, DNA profiles and fingerprints by law enforcement agencies, assessing their compliance with the obligations under the PoFA and under the Police and Criminal Evidence Act 1984 (PACE).[45]

2. Determining applications by the police to retain DNA profiles and fingerprints[46] (PoFA, Section 20(9)).

3. Reviewing national security determinations which are made or renewed by the police in relation to the retention of DNA profiles and fingerprints, with the ability to order that relevant material be destroyed (PoFA, Sections 20(3) to 20(5)).

4. Providing reports to the Home Secretary about the carrying out of the Commissioner's functions and any matter relating to the Commissioner's functions, (PoFA, Section 21).

5.51 Consequently, the scope of the Biometrics Commissioner is limited to law enforcement agencies and only concerned with certain types of biometric data. However, the ability of the Commissioner to report on any matter relating to its functions allows it to address topics beyond its immediate scope, such as the deployment of novel technologies by law enforcement agencies.

5.52 Under Section 29 of the PoFA, the Secretary of State must prepare a code of practice containing guidance about 'surveillance camera systems'. Section 34 of the PoFA established a Surveillance Camera Commissioner with a special remit relating to that code. The Surveillance Camera Commissioner has three primary functions:

45 The Protection of Freedoms Act 2012 (PoFA), Sections 20(2) and 20(6).
46 PoFA, Section 20(9).

1. Encouraging compliance with the Surveillance Camera Code of Practice.[47]

2. Reviewing the operation of the Surveillance Camera Code of Practice.[48]

3. Providing advice to Government ministers about the Code, including changes or it or breaches of it.[49]

5.53 'Surveillance camera systems' includes CCTV and any system for recording or viewing images for surveillance purposes.[50] It also extends to any other system associated with, or otherwise connected with CCTV and any other system for recording or viewing visual images for surveillance purposes.[51] This could therefore include a multitude of vision-based biometrics, within scope of the definition.

5.54 The Commissioner does not have enforcement functions or powers of inspection. It works with relevant authorities, including local authorities and police forces in England and Wales, to make them aware of their duty to have regard to the Code.[52] As part of the Commissioner's duties, it is responsible for providing advice on effective, appropriate, proportionate and transparent use of surveillance camera systems.

5.55 An example of the Surveillance Camera Commissioner's power to provide advice about the Code is the detailed opinion published in November 2020, on LFR, entitled: *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognitions Technology to Locate Persons on a Watchlist, in Public Places in England and Wales*.[53] Its recommendations gave particular emphasis on the

47 PoFA, Section 34(2)(a).
48 PoFA, Section 34(2)(b).
49 PoFA, Section 34(2)(c).
50 PoFA, Section 29(6)(a) to (c). It also includes Automated Number Plate Recognition, but that is not relevant to this Review.
51 PoFA, section 29(6)(d).
52 PoFA, section 33(5).
53 Surveillance Camera Commissioner. (2020). *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognitions Technology to Locate Persons on a Watchlist, in Public Places in England and Wales.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

importance of consistent ethical standards in the way such work is carried out.

5.56 Although the Surveillance Camera Code of Practice is only binding upon relevant authorities, the Commissioner has a responsibility to provide the surveillance camera industry with recommended standards.[54] The updated Code came into effect on 12 January 2022. The Commissioner's responsibilities towards the private sector extend to encouraging voluntary compliance with the Code.

5.57 The updated Code of Practice contains only two references to biometric technologies.[55] The first reference states no more than that such technologies must be justified, proportionate and for a stated purpose. It also states that they must also be 'validated', explaining that the Commissioner will validate systems. The amended Code now provides guidance for chief officers of police that want to use LFR to find people on watchlists. It recommends, amongst other things, that chief officers 'establish an authorisation process for LFR deployments and identify the criteria by which officers are empowered to issue LFR deployment authorisations'.[56]

5.58 In July 2020, the Government announced that the Biometrics Commissioner and Surveillance Camera Commissioner roles would be merged into a single appointment. The announcement prompted criticism from the existing post-holders and, the new office holder, Fraser Sampson, was appointed in March 2021. No new law has been introduced to circumscribe the new role and it is understood that the legal basis of the position will remain the same, but with a single person fulfilling all the relevant functions.

5.59 In addition, in September 2021, the Government suggested, in its consultation on the domestic data protection regime, that the dual roles of the Biometrics and Surveillance Camera Commissioner's

54 PoFA, Section 29(3).

55 Home Office. (2022). *Surveillance Camera Code of Practice,* paragraphs 2.4 and 12.3. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035067/Surveillance_Camera_CoP_Accessible_PDF.pdf

56 Home Office. (2022). Paragraph 12.3.

role could be absorbed into the ICO.[57] The Biometrics and Surveillance Commissioner subsequently expressed concerns that such a move would undermine the Commissioner's dual roles. In his view, neither role could be characterised as regulatory, whereas the ICO's was a statutory regulator.[58] It is unclear whether such a move would involve an amendment to the statutory foundation on which the Biometrics and Surveillance Camera Commissioner rests or if it would just mean a reallocation of resources.[59]

Forensic Science Regulator

5.60 The Forensic Science Regulator 'ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards'.[60] As Dr Tully, the post holder at the time of our interviews, explained in our evidence session, it is a broad remit with only a small overlap with biometrics. However, since some forensic science uses biometrics, and the Forensic Science Regulator sets quality standards that must be met in the use of forensic science in the criminal justice system, Dr Tully's role provides at least some regulation of the use of biometrics (for example, in setting standards for fingerprint or DNA comparison).

5.61 The Forensic Science Regulator has, since April 2021, existed pursuant to a statutory basis (Forensic Science Regulator Act 2021, Section 1). The Regulator now has a duty to publish a statutory code of practice (Section 2), as well as statutory powers to undertake investigations and issue formal notices (Sections 5 and 6).

57 Department for Digital, Culture, Media & Sport (DCMS). (2021). Data: A new direction, paragraphs 409 and 410. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf

58 DCMS. (2021). Section 6.

59 As this Review went to press, DCMS published its response to the *Data: A new direction* consultation, which proposes dissolving the Office of the Biometrics and Surveillance Camera Commissioner, and to distributing its functions to other regulators, potentially moving casework functions to the Investigatory Powers Commissioner and moving surveillance-related functions to the ICO. See: DCMS. (2022). *Data: a new direction – Government response to consultation*. Available at: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch5

60 UK Government. *Forensic Science Regulator*. Available at: https://www.gov.uk/government/organisations/forensic-science-regulator

The Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board

5.62 In 2018, the Home Secretary established an Oversight and Advisory Board in respect of LFR and new biometrics use by the police. Its membership was comprised of representatives from the police, the Home Office, the then Surveillance Camera Commissioner, the Information Commissioner, the then Biometrics Commissioner and the Forensic Science Regulator. The Court of Appeal in *Bridges* described the purpose of the Board as 'to co-ordinate consideration of the use of facial imaging and [Automated Facial Recognition] by law enforcement authorities'. In the conversations we had with relevant stakeholders, many referred, for example, to the Surveillance Camera Commissioner and Information Commissioner's roles in the oversight of LFR, but none made any mention of this Board. It last met in September 2019. The Gov.uk website asserts that 'alternative governance arrangements are now in place', but does not identify what those are.[61]

Biometrics and Forensics Ethics Group

5.63 The Biometrics and Forensics Ethics Group (BFEG) is an advisory, non-departmental public body, sponsored by the Home Office and comprised of experts in law, psychiatry, political theory, human geography, genetics and forensic science. It provides independent ethical advice to Home Office ministers on issues relating to the use of biometrics and forensics.

5.64 In December 2020, BFEG published 6 'Governing Principles' for the use of biometric, forensic and data analysis procedures:[62]

1. Procedures should enhance public safety and the public good.

2. Procedures should seek to respect the dignity of individuals and groups.

61 UK Government. *Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board'.* Available at: https://www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board

62 Biometrics and Forensics Ethics Group (BFEG). (2020). *Ethical Principles*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946996/BFEG_Principles_Update_December_2020.pdf

3. Procedures should not deliberately or inadvertently target or selectively disadvantage those most vulnerable people nor people or groups on the basis of protected characteristics as defined in the Equality Act 2010.

4. Procedures should respect, without discrimination, human rights as defined in the Human Rights Act 1998.

5. Scientific and technological developments should be harnessed to advance the process of criminal justice; promote swift exoneration of the innocent, and afford protection and resolution for victims.

6. Procedures should be based on robust evidence.

5.65 It has also published briefing papers addressing the ethical issues arising, for example, in relation to LFR use.[63]

63 BFEG. (2021). *Briefing note on the ethical issues arising from public– private collaboration in the use of live facial recognition technology.* Available at: https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible

6. The EU AI Draft Regulation

6.1 In April 2021, the European Commission published its proposed legal framework for the regulation of artificial intelligence ('AI').[64] While only a first draft, and therefore likely to be revised substantially during the trilogue process, it is an important reference that will set a benchmark against which other laws and regulations will be developed and measured. The proposal concerns AI in general, but makes express reference to certain forms of AI systems, such as biometric technologies, emotion recognition systems and social scoring systems.

6.2 It is no longer the case that EU law automatically becomes part of UK law. But just as the GDPR is now reflected in the UK GDPR, it seems highly likely that even after the UK has left the EU the legal regulation of AI and biometric data is likely to be highly influenced by, if not precisely mirror, EU law. As a result we considered it important to assess this attempt by the EU to set out a binding legal framework around AI including the processing of biometric data.

6.3 The proposed regulation takes a risk-based approach, with different rules applying to 'unacceptable-risk', 'high-risk', 'limited-risk' and 'minimal-risk' categories of AI. Into each of these categories fall different types of AI systems, as well as particular purposes for using AI.

6.4 Although the risk-based approach means that biometric technologies will generally be assigned to a risk category on a case-by-case basis, there are certain biometric identification technology uses which fall explicitly into the unacceptable and high-risk categories: remote biometric identification systems.

6.5 Throughout the proposal, the notion of biometric data is supposed to be interpreted in line with the definition under Article 4(14) of the

64 Council of the European Union. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act) and amending certain Union legislative acts*. 2021/0106 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:206:FIN

EU GDPR.[65] Much like under the GDPR, biometric identification systems are subject to more stringent requirements than biometric categorisation systems. Additionally, an important distinction is made between 'real-time' biometric identification systems and 'post' remote biometric systems. The latter are identification systems made after the biometric data has been collected and with a significant delay.[66]

'Real-time' biometric identification systems in publicly accessible spaces

6.6 The use of *real-time* biometric identification systems by law enforcement in publicly accessible spaces, such as LFR, falls into the category of unacceptable risk.[67] This is because it is seen as 'particularly intrusive'.[68] It is therefore *prima facie* prohibited,[69] although subject to explicit and inferred caveats.[70]

6.7 There are three explicit exceptions: where the use is strictly necessary for (1) targeted search for potential crime victims, including missing children; (2) the prevention of specific, substantial and imminent threats to life, for example terrorist attacks; or (3) the detection, localisation, identification or prosecution of a perpetrator or suspect of criminal offences referred to referred to in Article 2(2) of Council Framework Decision 2002/584/JHA, leading to a custodial sentence of over 3 years.

6.8 There are two implicit caveats of note. First, even when the prohibition to LFR was not subject to an exception, it would only apply where the technology is used in a publicly accessible space. As stated in Recital 9, 'publicly accessible' 'does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those

65 EU Artificial Intelligence Act, Recital 7.
66 EU Artificial Intelligence Act, Recital 37.
67 'Law enforcement authorities' has the same meaning as in Directive (EU) 2016/680 (the Law Enforcement Directive), (see: Article 3(40)).
68 Law Enforcement Directive, Recital 18.
69 Law Enforcement Directive, Article 5(1).
70 When law enforcement authorities use biometric technologies in private spaces, or use biometric technologies for purposes other than law enforcement, the category of risk assigned will depend on the type of biometric technology used and the purpose for which it is used.

parties have been specifically invited or authorised'. Whether a space is considered publicly accessible will be determined on a case-by-case basis.[71]

6.9 The second caveat concerns the scope of the provisions relating to high-risk biometric identification systems. Recital 2 states that the basis in EU law for these provisions is Article 16 of the Treaty on the Functioning of the European Union (TFEU). Article 16 of the TFEU limits the scope of EU law and Member States' national security is a paradigm example of activity that falls outside the scope of EU law.[72] Consequently, where law enforcement uses biometric technologies in the context of national security, the proposed regulation would not apply. We consider this to be particularly problematic, given that the use of biometric technologies for national security purposes was identified by the former Biometrics Commissioner as giving rise to considerable concern due to a lack of adequate oversight.[73]

6.10 Where law enforcement is permitted to use biometric technologies in publicly accessible spaces for one of the aforementioned purposes, the use is still subject to further constraints. First, the use must be limited and proportionate, taking into account the seriousness, likelihood and scale of potential harm caused in absence of the use of the technology, as well as the rights impact caused by using the technology.[74] In addition, prior authorisation must be given by a judicial or independent authority.[75] This function is more akin to the role played by the Investigatory Powers Commissioners than this Review's proposed national Biometrics Ethics Board. Finally, Member States must implement national legislation concerning the use of real-time biometric technologies by law enforcement in publicly accessible spaces prior to its use.[76] That legislation can be more restrictive than the proposed regulation by only allowing it for some of the three explicit situations.

71 EU Artificial Intelligence Act, Recital 9.
72 Treaty on European Union, Article 4.
73 Biometrics Commissioner. (2020). *Annual Report 2019*, chapter 4. Available at: https://www.gov.uk/government/publications/biometricscommissioner-annual-report-2019
74 EU Artificial Intelligence Act, Article 5(2).
75 EU Artificial Intelligence Act, Article 5(3).
76 EU Artificial Intelligence Act, Article 5(4).

Biometric identification systems

6.11 Both *real-time* and *post* remote biometric identification systems are categorised as high-risk.[77] In order to 'mitigate the risks for health, safety and fundamental rights',[78] high-risk biometric technologies are subject to several requirements. There are three of particular note.

6.12 First, high-risk biometric technologies must undergo an *ex ante* conformity assessment, which must be carried out by a designated testing authority.[79] The conformity assessments extend to an examination of source code, where necessary.[80] The conformity assessment explores issues such as statistical bias, which must be mitigated in the training and testing of datasets of high-risk biometric systems.[81]

6.13 Secondly, both real-time and post remote biometric identification systems must be designed and developed in a way that enables human oversight and intervention while the system is in use.[82] The Surveillance Camera Code of Practice already mandates human intervention before a decision is made based on the output of a facial recognition system.[83] The rationale is that it mitigates the likelihood of a false positive occurring on the basis of a wholly automated decision.[84] However, there may be edge cases where mandatory human intervention inadvertently precludes an individual's right to object to a decision made based solely on an automated decision under the EU GDPR.[85] Nonetheless, the benefit caused by mandating the opportunity for human oversight may outweigh the detriment suffered by individuals unable to exercise their right to not be subject to a decision based on solely automated processing.

77 Annex III to the Proposal for a Regulation of the European Parliament and of the Council, Section 1.
78 EU Artificial Intelligence Act, Recital 43.
79 EU Artificial Intelligence Act, Articles 19 and 43.
80 EU Artificial Intelligence Act, Article 64(2).
81 EU Artificial Intelligence, Article 10(3).
82 EU Artificial Intelligence Act, Article 14.
83 Home Office. (2013). *Surveillance Camera Code of Practice*, paragraph 3.2.3. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055736/SurveillanceCameraCodePractice.pdf
84 *Bridges*, paragraph 184.
85 EU GDPR, Article 22(1).

6.14 Thirdly, providers of 'high-risk' AI systems have to implement a quality management system that, amongst other things, involves testing and validation procedures to be carried out before, during and after development.[86] In parallel, users of high-risk biometric technologies must monitor the use of the system for problems, passing on information to providers where they are identified.[87] Concerningly, these measures seem to be aimed at issues inherent in the technology, rather than also seeking to mitigate problems that might arise due to the way an AI system is used. For example, there doesn't appear to be any oversight or mitigating actions to prevent harm caused due to users of high-risk biometric systems deviating from a provider's recommended false positive rate, thereby increasing the likelihood wrong identification. An example of the issues that can arise has been demonstrated by the ACLU,[88] which ran a test on US Congress members using Amazon's Rekognition facial recognition technology with a confidence threshold set below the recommended level,[89] misidentifying 28 members of Congress as criminals, and disproportionately providing false matches for Black and Latinx lawmakers.

6.15 It is also worth noting that the proposal clarifies that the condition for processing special category data under Article 9(2)(g) of the EU GDPR ('necessary for reasons of substantial public interest') includes the purposes of bias monitoring, detection and correction.[90] Any processing must include safeguards for fundamental rights, including technical limitations on the reuse of processing.

86 EU Artificial Intelligence Act, Article 17(1).
87 EU Artificial Intelligence Act, Article 29(4).
88 American Civil Liberties Union.
89 Ghaffray, S. (2019). 'How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement'. *Vox*. Available at: https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation
90 EU Artificial Intelligence Act, Article 10(5).

Biometric categorisation systems

6.16 Unlike biometric identification systems, biometric categorisation systems do not fall expressly into the risk categories. Therefore, determining where such systems fall on the risk spectrum will be undertaken on a case-by-case basis. Nonetheless, there are transparency notifications that apply to biometric categorisation systems.[91] Those deploying such systems must make clear to data subjects that the subject is being categorised, except where they are permitted by law to detect, prevent and investigate criminal offences.[92] These exceptions reflect the permitted derogations when an individual wishes to exercise their rights under Part 3 of the DPA 2018.

6.17 The proposal also intends for voluntary codes of conduct to be drawn up, which would apply to AI systems[93] other than high-risk AI systems, which would include biometric categorisation systems.

6.18 The potential rights impact caused by biometric categorisation systems can be equal to the potential rights impact caused by biometric identification systems. Therefore drawing a distinction between the two appears to be artificial and it is difficult to discern a clear basis for the proposed regulation holding that lower transparency requirements and self-regulation are considered adequate protections for biometric categorisation systems. There appears to be little justification for not deeming biometric categorisation systems as high-risk, thereby subjecting them to the more onerous obligations of high-risk AI systems.

6.19 On 29 November 2021, the Council of the European Union published its compromise text of the Act (i.e. a response to the original text). One notable amendment was the suggestion that biometric systems be defined as high-risk where such systems are 'intended to be used for the "real-time" and "post" biometric identification of natural persons without their agreement'.[94]

91 EU Artificial Intelligence Act, Article 52.
92 EU Artificial Intelligence Act, Article 52(2).
93 EU Artificial Intelligence Act, Article 69(1).
94 Council of the European Union. (2021). *Presidency Compromise Text*, Annex III, paragraph 1. 2021/0106 (COD). Available at: https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf

6.20 Such a change would seemingly increase the scope of biometric systems considered high-risk, as the amended definition applies irrespective of whether the identification is taking place remotely, and requires consent to have been obtained for a system to be defined as not high-risk. However, it is important to note that it is currently not clear whether any such amendments will be adopted in the final text of the Act.

7. Evidence

The current legal framework and what regulation should look like

7.1 None of the individuals with whom we spoke thought that the current legal framework was fit-for-purpose, though there was a considerable divergence of views over what an improved framework should look like. This ranged from those who believed fundamental change was essential and others who believed that imminent changes would be sufficient to rectify existing deficiencies.

7.2 Liberty and Big Brother Watch, for example, both consider that a fit-for-purpose legal framework would have to include an outright ban on the use of LFR – a technology which they consider causes 'unmitigable' human rights issues. That approach has been adopted, for example, in California, which in 2019 introduced a 3-year ban on the use by law enforcement agencies of LFR,[95] and Amazon, IBM and Microsoft have also announced the suspension of sales of LFR technology to police forces.[96] Following our evidence sessions, in August 2021 over 30 human rights organisations published an open letter calling on the UK Government to ban the use of LFR in public.[97] A non-binding resolution banning the use of LFR in public by police was also overwhelmingly approved by the European Parliament in October 2021.[98]

95 Paulson, E. (2019). 'California bans police use of facial recognition for three years'. *ITPro.* Available at: https://www.itpro.co.uk/policy-legislation/34603/california-bans-police-use-of-facial-recognition-for-three-years

96 Paul, K. 'Amazon to ban police use of facial recognition software for a year'. *The Guardian.* Available at: https://www.theguardian.com/technology/2020/jun/10/amazon-rekognition-software-police-black-lives-matter; Dastin, J. and Vengattil, M. (2020). 'Microsoft bans face-recognition sales to police as Big Tech reacts to protests.' *Reuters*. Available at: https://www.reuters.com/article/us-microsoft-facial-recognition-idUSKBN23I2T6; BBC News.(2020). 'IBM abandons '"biased" facial recognition tech.' Available at: https://www.bbc.co.uk/news/technology-52978191

97 Privacy International and other Civil Society Groups. (2021). *Live Facial Recognition Technology should not be used in public spaces*. Available at: https://privacyinternational.org/sites/default/files/2021-08/LFRT%20Open%20Letter%20Final.pdf

98 European Parliament. (2021). *Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*. 2020/2016(INI)). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

7.3 Government ministers, Baroness Williams and Kit Malthouse MP emphasised to us their 2019 manifesto commitment for police use of biometrics and the need to introduce a legal framework to 'put it beyond doubt that we are operating in a legal manner', but were less clear as to how that would be done. Others felt that the intrusive impact of such technology could, at least, be tempered by an improved legal framework (as well as accuracy improvements – on which see further at 7.26. below).

7.4 Notwithstanding these differences, there was almost complete consensus that new legislation is necessary in this field. While Lindsey Chiswick, Director of Security in the Metropolitan Police Service, considered that the introduction of guidance to govern the use of LFR would be sufficient to provide an adequate legal framework, most interviewees felt that a statutory footing for the use of intrusive biometric technologies was a necessary development in the field. Dr Daragh Murray, for example, observed that reliance on the common law 'could lead to arbitrariness', with the current framework 'not currently sufficiently clear to guide activity', and the then Surveillance Camera Commissioner described himself as 'unimpressed that the police believed all they needed to do was publish guidance'. Some police experts, however, are in favour of legislation: Detective Chief Superintendent Chris Todd of West Midlands Police underscored how difficult the current legal framework is for the police to apply operationally: 'the [existing] legislation was written before relevant technologies were normalised. In the absence of any specific regulatory framework, the police are having to work with that legislation and guidance and take a case-by-case basis.' That clearly increases the scope for error and arbitrariness which could be addressed by legislation. Interviewees did note that existing duties under the HRA, Equality Act, and the DPA 2018 were useful and ought to be maintained in the next phase of biometric regulation.

7.5 In terms of the substance of a new legal framework, the predominant view expressed to us was that it ought to be technologically neutral and that it should not only take account of the type of data in issue (e.g. personal data), but also the purpose for which data was collected or used and the degree of interference with personal rights. That would enable legislation to take what Amba Kak of AI Now described as 'a risk-based approach', recognising the prevailing view that 'the most pernicious

uses of biometrics [at present] are LFR and the least pernicious are 1:1 matching.'

7.6 In terms of the procedure or permissions which would be necessary for the use of biometrics, most interviewees rejected the idea of a warranty system (by which specific authorisation via warrants would be necessary before biometric technologies could be deployed). They considered it to be too cumbersome and opaque, and we had particular interest in the views of those, such as police, who would have to work with such warranty requirements. They highlighted that much can be achieved by co-operation and dialogue to ensure 'improved working practices and organisational standards that demonstrate regard for human rights principles'.[99] There was significant agreement to the need for certain procedural steps (such as accuracy testing or impact assessments) to be conducted in order for deployments to be lawful; but most interviewees had not given much thought to exactly what new legislation ought to look like. Robin Allen QC and Dee Masters from AI Law Hub noted that a weakness with the current system is that it permits claims to be brought once there has been a breach of a legal rule (for example, of the HRA or Equality Act) but does not provide sufficient prior protection to prevent those breaches from occurring. We were strongly persuaded that this is something that a new legislative framework should attempt to address. We agree, and the capacity to put in place safeguards prior to deployment is considered elsewhere, including under Recommendation 8.

7.7 All witnesses thought that legislation would have to be supplemented by guidance and codes of practice to provide comprehensive governance. The former Surveillance Camera Commissioner described the Surveillance Camera Code of Practice as 'very weak and old … a new regulator would need an up-to-date Code of Practice to provide new guidance'.[100] The Centre for Data Ethics and Innovation (CDEI) observed that 'many groups have called for a Code of Practice to strengthen governance of police deployment' of biometrics; and the evidence we took from the Metropolitan Police, West Midlands Police, and the College of

99 Elaine Scott and David Hamilton from Police Scotland. A very similar view was expressed by the former Biometrics Commissioner.
100 This is reflected in the fact that the first major amendment to the Code since 2013, was published in August 2021.

Policing confirmed that police stakeholders also see the need for additional guidance to be introduced to ensure, in the words of Chris Todd of West Midlands Police, 'consistency across forces'.

The Court of Appeal judgment in *Bridges*

7.8 We asked all witnesses about the Court of Appeal judgment in *Bridges*. We were surprised by the very different interpretations they had of the judgment – in particular, the view of some witnesses, including Government ministers, that the Court of Appeal had said that South Wales Police's use of LFR was lawful when, in fact, the Court found the opposite.

7.9 This misunderstanding seems to have arisen in two ways, First, the Court of Appeal found that the police have a common-law power to use LFR. That was interpreted by some witnesses as meaning its use was lawful. The important error here, is that the Court of Appeal found that, while there was a common-law source of the power, the exercise of that power was not 'in accordance with law' for the purposes of Article 8 of the European Convention on Human Rights (ECHR). This was because there was an insufficient legal framework to protect individual rights: the legal framework did not comply with the required standards of accessibility and foreseeability. That made the exercise of the power unlawful. It is a fundamental legal principle that the existence of a power does not automatically mean that its exercise is lawful. But that distinction appears to have been overlooked by some witnesses.

7.10 Secondly, others seemed to think that, because the Court of Appeal did not find that South Wales Police had 'broken' any law, the use of LFR was lawful. Again, that overlooks the Court of Appeal's finding that there was no adequate legal framework in place, and insufficient impact assessments had been performed. Those failures rendered the use of LFR *unlawful*.

7.11 If an appropriate legal framework is to be introduced, the deficiencies in the current legal framework must be frankly addressed. We were concerned about the lack of understanding displayed among those, including lawmakers, who will have a role in determining a future legal framework as to what has been deemed to be deficient in the existing system.

7.12 Notwithstanding the above, many witnesses (including police witnesses) described the *Bridges* judgment as 'useful' in setting the parameters within which further development of the law around LFR can occur. Some were disappointed that the judgment did not go far enough. For example, Liberty (who were involved in the case) were disappointed that the Court of Appeal overlooked the impact of a privacy intrusion that occurs on groups or categories of people when LFR is deployed on crowds. Instead it assessed the impact of LFR on the rights of individuals, which the Court of Appeal then considered to be limited because of the automatic deletion of individual images. Liberty believed this was a misunderstanding of the nature of the interference with privacy rights caused by LFR and how its necessity, proportionality, and other purported justifications, as well as its discriminatory impact, should be assessed.

Oversight and regulators

7.13 There was near unanimity that oversight and regulator structures are unclear, fragmented and confusing. We were struck how the need for clear and firm guidance was sought by all the interviewees even when their views differed on other issues. Police witnesses, for example, described how difficult it was to know who to go to for advice or guidance. Regulators themselves described how their functions overlapped risked confusion or gaps in the overall framework.

7.14 The former Biometrics Commissioner and Surveillance Camera Commissioner were frank about their experiences of the roles. We were especially grateful to them for their candour. The former Biometrics Commissioner wondered whether the commissionership 'does the job legislators intended' because it is 'too easy to side-line and there are no obligations on relevant bodies in Parliament or in Government' to meet with or take the Commissioner's recommendations into account. The former Surveillance Camera Commissioner noted that 'surveillance takes many modalities' with biometrics being 'an important aspect but not the sole issue'. Conflict over the scope of their respective roles had not been a problem because of the good working relationship between the two Commissioners, but we heard from various witnesses that the distinctions and overlaps between the

Biometrics Commissioner, Surveillance Camera Commissioner and Forensic Science Regulator could be problematic in terms of the transparency and legitimacy of regulation. Suzanne Shale who chairs the London Policing Ethics Panel described the Panel as having been 'struck' by 'regulatory confusion regarding who has competence to look at these issues'. The former Forensic Science Regulator identified some areas – such as the use of biometrics in the family courts – over which none of the existing regulators appear to have jurisdictional competence. Fragmentation exists at ministerial level too, with Baroness Williams responsible for biometrics but Kit Malthouse MP responsible for facial matching.

7.15 The ICO's evidence was that it is empowered and competent to act as the regulator of biometrics. Other witnesses were less confident that this was or would be an effective arrangement. They emphasised that since the ICO has general jurisdiction over 'data processing' and 'because the world is increasingly data driven, the ICO could have an unlimited remit'. This may be damaging to democratic engagement and control,[101] and the ICO's focus on individual privacy might cause the group privacy concerns associated with biometrics to be overlooked.[102]

7.16 There were some positive comments about the approach adopted in Scotland, where the Biometrics Commissioner (a role established in 2020, with Dr Brian Plastow announced as the first Commissioner in March 2021) has greater independence, being appointed by the Scottish Parliament rather than the executive. That role has a clear remit to draw up a Code of Practice to meet principles legislated for by the Scottish Parliament. It was 'a good method of governance', in the view of the outgoing England and Wales Biometrics Commissioner.

Ethics

7.17 We had useful conversations about ethics with various witnesses. Under Chris Todd, West Midlands Police has developed a Digital Ethics Panel to which all considerations of new technologies

101 Evidence of the Surveillance Camera Commissioner.
102 Evidence of the Biometrics Commissioner.

are referred for advice; but that is a local arrangement not yet replicated in other forces. Suzanne Shale found it 'striking to see how little ethical scrutiny there was of trials of policing technologies of the population'. Having come from a health background, where ethical considerations are embedded in practice, she thought that a similar approach could work in relation to biometrics. It was her view that underlying good practice, 'there are a set of choices on how to conduct oneself and promote ethical behaviour.' An Ethics Panel can help with those ethical judgments.

7.18 While we had sought to interview members of the Biometrics and Forensics Ethics Group (BFEG), in the event we were unable to arrange an interview. We have, however, taken account of their useful publications. In considering the issue of ethics with those we did interview, we were struck that very few were aware of, or volunteered information relating to, BFEG. In our view, this was indicative of the limited remit BFEG has been given to advise the Home Office rather than to provide broader ethical guidance to those deploying biometric technology.

7.19 Overall, we found considerable support for the creation of a national biometrics ethics group, in particular in relation to police use of biometrics. Chris Todd was keen for the West Midlands model to be expanded nationally, and the College of Policing also considered that 'the concept of a national ethics body is a good thing'. Suzanne Shale highlighted the benefit that can accrue from 'externality, especially with historically closed institutions' but warned that 'externality can be weak because it can be easy to ignore the advice.'

7.20 Taking this into account, we asked interviewees two important questions about an independent Biometrics Ethics Board in practice:

1. Should an independent Ethics Board have a *mandatory* remit? Planned uses of biometric technology (particularly by the police but also, potentially, by other bodies including private bodies) would be legally required to undergo scrutiny by the Board before deployment against the public.

2. Should an independent Ethics Board have the *right to veto* deployments or merely an advisory-only role?

7.21 For the avoidance of doubt, we made clear that on both proposals – mandatory referral and the more extreme step of the power of veto – any rules may be subject to exceptions such as public emergencies, or agreement by the Ethics Board that scrutiny was unnecessary.

7.22 Views on these questions were mixed.

7.23 On mandatory referral of new biometric technology for consideration by an Ethics Board before deployment, most of those who worked in or with policing were opposed to it. Lindsey Chiswick from the Metropolitan Police Service did not think mandatory referral was necessary because the police would want an Ethics Board's insight and so would make voluntary referrals; that view was echoed by the College of Policing. We queried this position on the basis that if it was correct, mandatory referral should be of no detriment to the police: it would merely be mandating what they wanted to do anyway. But, in further discussion there appeared to be a point of principle in play as to whether the decision to make a referral to an Ethics Board should always be a voluntary process for the police to engage, rather than one the police should be required to go through. This caused us to contemplate how effective an Ethics Board would be, if referrals to it were left entirely to the discretion of the very public authorities it was there to scrutinise.

7.24 Additionally, the Metropolitan Police had practical concerns that mandatory referral to an Ethics Board would add 'more hoops to jump through' which 'may not achieve better policing'. Suzanne Shale thought it would be difficult to formulate a schema for mandatory referral to the London Policing Ethics Panel – but that Panel's focus is broader than biometrics (it oversees *any* ethical issue arising in policing) and that difficulty may, therefore, be easier to overcome for a biometrics-specific Ethics Board.

7.25 On the question of whether such a Board should be able to impose a binding veto on the use of new biometric technology, there was a general consensus that it should be advisory. However, the College of Policing was prepared to contemplate that there might be 'exceptional circumstances' in which it could veto a planned use.

Accuracy and bias

7.26 Accuracy and bias were two of the most frequently cited concerns with biometric technology, along with the associated risks of privacy intrusion and power imbalances.

7.27 It was recognised that bias can arise in multiple ways in the deployment of biometric technologies: it may be inherent to the technology, or it may accrue in the manner in which it is used (reflecting, for example, existing bias in policing practices who have disproportionate engagement with particular communities).

7.28 One acute example of bias in biometric technology is the apparent embedding of race and sex bias in the computer vision software tools that facial recognition developers use. MIT researchers found that commercial face classification algorithms performed better on male than on female faces, and also on lighter than on darker ones with an error rates of up to 35% for darker female faces. That compares with an error rate for white male faces of 0.8%, at highest.[103] Similar findings have been made in tests of commercial facial recognition systems (for ID pictures, not video cameras) where all of these had biased performance for various characteristics including skin reflectance, gender, age and even height.[104]

7.29 Bias in biometric technology is often also caused by statistical bias. An example of statistical bias is selection and sampling bias, where a dataset does not reflect the subjects being scrutinised. In evidence to us, the former Biometrics Commissioner argued that the use of biometric technologies should reflect the demographics of the population that will be subject to it, which 'could mean the UK population or it could mean the population of an area of interest to the police'. Accuracy bias may be improved by, for example, analysing and reviewing the datasets which are used,[105] leading

103 Buolamwini, J. and Gebru, T. (2018). 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency. Proceedings of Machine Learning Research*, 81: pp. 77-91.

104 Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L. and Vemury, A. R. (2019). 'Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems'. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, pp. 32-41. doi: 10.1109/TBIOM.2019.2897801.

105 Evidence of Detective Chief Superintendent Chris Todd, West Midlands Police.

to fewer automated false positives and false negatives. For the former Forensic Science Regulator, 'the key part of standards in relation to discrimination is the requirement to scientifically test and understand the implications of what you are doing.' In the same vein, the former Surveillance Camera Commissioner recommended that unless bias is removed or significantly reduced, police forces should continue to carry out context-specific trials and continue to monitor the results. This is not straightforward: one of the challenges in addressing bias is that some rights-protecting safeguards (for example, the immediate deletion of data by LFR systems where no positive match to a watch list is made) inhibit the possibility of *post-facto* bias analysis. This is because the deleted data cannot be checked or assessed to ascertain any bias in the operation of the system. That does not mean that material should be retained (indeed, to do so might violate data protection law), but it highlights the difficulties in overcoming bias in facial recognition technology, and the acute need for testing and protection against discrimination to be rigorously performed prior to a system's deployment. Other proposals for reducing bias in facial recognition technology include: improving diversity in training datasets; mandatory standards for accuracy; higher quality photo capture; and tailoring of threshold settings to different demographics to ensure greater accuracy. [106]

7.30 However, in the view of some interviewees, even if accuracy bias is overcome, 'there are wider discriminatory issues' which cannot be overcome.[107] In Liberty's view, remedying accuracy deficiencies in biometric technologies would merely lead to 'the perfection of surveillance technology', which would continue to have a significant detrimental impact on individual rights. The former Biometrics Commissioner reasoned that 'it's important to make sure that biometric technology doesn't make worse the discriminatory problem it was supposed to address.'

106 Mclaughlin, M. and Castro, D. (2020).'The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist'. *Information & Technology Innovation Foundation.* Available at: https://itif.org/sites/default/files/2020-best-facial-recognition.pdf

107 Evidence of Silkie Carlo, Big Brother Watch and Megan Gould, Liberty.

Taking account of public opinion

7.31 We asked interviewees for their views on the extent and manner in which public opinion could validly inform the regulation of biometric data. This included the extent to which public consent, or tacit assent, to data collection and processing could supersede legal protections that might otherwise be in place. This was of interest to us for a number of reasons. First, because public authorities often seek to justify their approach to privacy by reference to a perception of what the public would be willing to accept in a balance between achieving particular goals – such as the prevention of crime – and reducing their right to biometric data privacy. Second, because if such public opinion is relied upon, the technical nature of the area in question, in combination with the complex intrusions of personal freedom that biometrics can occasion, makes informed public engagement difficult.

7.32 Most of those from whom we took evidence agreed there are real challenges in public engagement and public understanding of the risks of biometric technology use. The police interviewees were clear that policing rests on democratic legitimacy and that public understanding and consent is therefore crucial.

7.33 The Government ministers with whom we spoke considered that this was adequately addressed by the inclusion in a manifesto of biometric-related commitments. An election victory itself provided the necessary endorsement of proposed biometric data use by public authorities and the extent to which they might intrude on privacy protections.

7.34 Others took a more nuanced approach. Liberty recognised the 'inherent dangers with allowing the public to determine the outcome of these issues, since they are complex and can be misunderstood'. The CDEI also warned about the need to 'be wary of following majority opinion where minority groups may be more affected than the majority.'

7.35 The former Surveillance Camera Commissioner considered that 'there has been no proper informed consent in relation to the deployment of biometric technologies so far. The public do not fully appreciate the ways in which biometric technologies work or the

implications of their deployment – there needs to be better public engagement.'

7.36 The ICO thought that citizen councils might be an appropriate means of ensuring sufficient understanding underpinned any public opinion that would then influence policy-making. On this latter point we benefited from the Ada Lovelace Institute convening such councils while we were conducting our research. They led to a series of thoughtful recommendations being proposed.[108]

7.37 The democratic legitimacy element of public engagement was also important for Big Brother Watch who thought that, nevertheless, public opinion 'doesn't necessarily have to inform the structure of regulation'.

7.38 Few interviewees demurred from what we believed to be the starting point of our analysis in this area: public engagement is essential, and insofar as it can be determined, understanding public opinion is important. But ultimately the determination of how law and regulation protects fundamental rights is to be determined by legislators and regulators.

108 Ada Lovelace Institute. (2021). The Citizens' Biometrics Council. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

8. Recommendations

8.1 Taking account of all the views expressed by those with whom we talked, as well as extensive research from expert bodies in the public domain, we have formulated 10 recommendations for the development of the governance of biometric data in England and Wales.

Recommendation 1: The need for a new legislative framework

8.2 First, we recognise that there is an urgent need for a new legislative framework specifically addressing and making provision for the regulation of biometric data.

8.3 This recommendation responds to, and endorses, the growing awareness (not just in the UK) that legislation is necessary as the starting point for governance of biometric data, in order to ensure a clear, accessible and rights-compliant basis for regulation and use of biometric technologies. The need for legislation has become clearest, perhaps, in the context of uses of LFR: the *Bridges* judgment pointed to the inadequacy of the current legal framework for police use of LFR, and the former Surveillance Camera Commissioner, in evidence to the Review, made clear that the problem with mass deployment of biometrics, and particularly live facial recognition, goes beyond law enforcement. Vendors of CCTV systems now offer facial recognition as standard and many public and private organisations have to make a decision on whether to enable the facility.[109] Some companies such as Microsoft have called for specific legislation on facial recognition. The company states plainly that the 'use of facial recognition technology could unleash mass surveillance on an unprecedented scale' and wants to avoid a commercial race to the bottom on rights by creating

109 Sabbagh, D. (2019). 'Lack of guidance leaves public services in limbo on AI, says watchdog'. *The Guardian*. Available at: https://www.theguardian.com/technology/2019/dec/29/lack-of-guidance-leaves-public-services-in-limbo-on-ai-says-watchdog

a level playing field.[110] The European Data Protection Supervisor has noted that 'in the absence of specific regulation so far, private companies and public bodies in both democracies and authoritarian states have been adopting [LFR] technology for a variety of uses. There is no consensus in society about the ethics of facial recognition, and doubts are growing as to its compliance with the law as well as its ethical sustainability over the long term.'[111]

8.4 The prominence of LFR in public debate at the moment should not, however, cloud the fact that the same principles will apply, and the same risks are likely to emerge, from the development and use of other biometric technologies. Indeed, the witnesses with whom we spoke recognised that other technologies (some not yet fully developed) could be equally rights-intrusive and that legislation should, so far as possible, be technologically neutral to account for future developments as well. Legislation would therefore need to be procedure and principle-setting, rather than use-specific. The police and public authority witnesses with whom we spoke also generally embraced the need for legislation, recognising that democratic legitimacy and their operational capacity would be improved by clear statutory rules setting out the way in which biometric technology could be used.

8.5 In June 2021, the Prime Ministerial Taskforce on Innovation, Growth, and Regulatory Reform, known as TIGRR, published a wide-ranging report on future regulation for the UK. It included proposals to replace the UK GDPR with a novel 'UK Framework of Citizen Data Rights' in order to 'cement [the UK's] position as a world leader in data'.[112] That new framework would be 'based more in common law', which is contrasted with the 'prescriptive' and 'inflexible' UK GDPR.[113] It has an emphasis on reforming the data protection regime in order to 'boost innovation'. Although the proposals are high level and occasionally conflicting, it is worth noting that Oliver Dowden MP, the then Secretary of State for Digital, Culture, Media and Sport indicated a desire to amend

110 Smith, B. (2018). 'Facial recognition: It's time for action'. *Microsoft On the Issues*. Available at: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

111 Wiewiórowski, W. (2019). 'Facial recognition: A solution in search of a problem?'. *European Data Protection Supervisor*. Available at: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

112 Taskforce on Innovation, Growth, and Regulatory Reform (TIGRR). (2021). *Independent Report*, paragraph 204. Available at: https://www.gov.uk/ government/publications/taskforce-on-innovation-growth-and-regulatory-reform-independent-report

113 TIGRR. (2021). Paragraphs 206–207.

the current data protection regime. As he said in a recent policy paper, 'the UK now controls our own data protections laws and regulations'[114] and can therefore remove what the Government sees as 'unnecessary barriers to data use'. That suggests a potential move towards the liberalisation of standards required for the use of biometric data,[115] rather than the introduction of stronger safeguards. In our view this would be inconsistent with what the regulatory landscape requires and what we heard from most of the witnesses who gave evidence to us. Indeed, we also do not see that such a move away from the standards contained in GDPR would be possible, because of the importance of the GDPR to international data protection. If we intend to maintain any cross-border data transfer co-operation with the EU, we will have to meet the minimum standards of the GDPR. In our view any TIGRR proposals to the contrary are unlikely to be adopted.

8.6 Calls for the introduction of new legislation are happening globally. In October 2020 the Global Privacy Assembly, composed of a majority of the world's data protection authorities, adopted a resolution on facial recognition technology that reiterated the importance of 'legal frameworks that are fit for purpose in regulating evolving technologies such as facial recognition technology'.[116]

8.7 In the United States, the AI Now Institute, a world-class policy research centre at based at New York University (whose Director of Global Policy gave evidence to the Review), has addressed some of the constraints of existing data regulation as the source of biometric regulation:

'While data-protection laws have made fundamental shifts in the way companies and government approach the collection, retention, and use of personal data, there are clear limitations on their ability to address the full spectrum of potential harms produced by new forms of data-driven technology, like biometric

114 DCMS. (2021). *Digital Regulation: Driving growth and unlocking innovation*. Available at: https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation#our-digital-regulation-principles

115 DCMS. (2021).

116 Global Privacy Assembly. (2020). *Adopted resolution on facial recognition technology*. Available at: https://edps.europa.eu/sites/default/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf

identification and analysis.'[117]

8.8 This is in part because data protection laws focus on 'individual (rather than group) conceptions of harm [which] fails to meaningfully address questions of discrimination and algorithmic profiling'.[118] This was also a concern we heard from Big Brother Watch, particularly when discussing the *Bridges* judgment. The use of existing sources of law, both data protection and human rights law, as the entry point for biometric governance, fails to take into account some of the specific features and specific risks posed by biometrics, particularly on the group level.

8.9 A new English statutory framework need not attempt to solve these issues in isolation, but can tackle lacunae in existing law by drawing on developments taking place elsewhere. Legislators in the United States have proposed several bills to address the need for specific biometrics regulation. The Algorithmic Accountability Act 2020 would have required entities that use, store, or share personal information to audit and conduct impact assessments for 'high-risk' automated systems, including those that can generate discriminatory outcomes.[119] An updated Act has recently been reintroduced, containing similar provisions to the previous iteration.[120] The No Biometric Barriers to Housing Act[121] would ban the use of biometric recognition technology in some dwelling places, while the Commercial Facial Recognition Privacy Act 2019[122] strengthens transparency requirements and consent in that context. The European Parliament and the European Commission have detailed ongoing projects to regulate the both the use of artificial intelligence generally and the use of biometric data, in particular.

117 Kak, A. (ed.). (2020). *Regulating Biometrics: Global Approaches and Urgent Questions.* AI Now Institute. Available at: https://ainowinstitute.org/regulatingbiometrics.html

118 Kak, A. (ed.). (2020).

119 Algorithmic Accountability Act, H.R.2231, 116th Cong. (2019) <https://www.congress.gov/bill/116th-congress/house-bill/2231>

120 Algorithmic Accountability Act 2022 <https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202022%20Bill%20Text.pdf>

121 No Biometric Barriers to Housing Act, H.R.4008, 117th Cong. (2021) <https://www.congress.gov/bill/117th-congress/house-bill/4360?s=1&r=87>

122 Commercial Facial Recognition Privacy Act, S.847, 116th Cong. (2019) <https://www.congress.gov/bill/116th-congress/senate-bill/847>

8.10 In our view the new legislation should make provision for four stages of biometric technology development: (i) testing, (ii) piloting, (iii) use and (iv) evaluation. Before any testing, piloting or use on members of the public, legislation should, at minimum, make provision for specific procedural duties that must be satisfied:

1. The conduct and publication of an equality impact assessment, following the requirements imposed by Section 149 of the Equality Act 2010 but strengthening that requirement by requiring publication of the assessment to ensure transparency.

2. The conduct and publication of a privacy impact assessment, which should consider the individual and group privacy rights ramifications of the intended deployment.

3. An accuracy assessment, by which the technological specifications and performance of the technology (including, for example, the particular software to be deployed) is assessed.

4. A necessity and proportionality analysis, requiring up-front consideration by the intended user of a biometric technology whether that use is (i) necessary in pursuit of a legitimate aim and (ii) proportionate, including whether a less intrusive means of pursuing the legitimate aim could be used and whether a fair balance will be struck between the various rights and interests at stake.

5. Where the intended user is a public body, mandatory referral to an Ethics Board (see Recommendation 7).

8.11 There are two further features of a new legislative framework that are of critical importance.

8.12 First, the introduction of a new legal framework should *simplify* rather than complicate, the existing patchwork of statutory bodies overseeing the law and regulation of biometric data. We were struck by numerous witnesses expressing concern over potential confusion over which commissioner or regulator had key responsibility over the safeguards relating to a new technology and how overlapping roles were resolved. This is important in relation to Recommendation 3, below, on the importance of clear codes of practice. In the absence of a clearer oversight structure, the

numerous codes of practice or guidance notes issued by different public authorities at various times create confusion, rather than clarity.

8.13 Second, the new legal framework should include a mechanism for prior authorisation – or at least prior consultation – with a statutory body prior to the use of new biometric technology, or existing technology in a new way. This would overcome the problem identified by Robin Allen QC and Dee Masters, namely that the current legal framework only provides for legal action vindicating individual rights to be brought once there has been a breach of those rights. Authorisation and/or consultation prior to use would also inform risk assessments and ultimately, judgments on proportionality.

Recommendation 2: The statutory framework should cover use of biometric data for identification and for classification

8.14 All biometric data is personal data because it is data that allows or confirms the unique identification of an individual. However, as discussed at paragraph 5.15, under UK GDPR, Article 9, biometric data is only classified as special category data when it is processed for the purpose of uniquely identifying an individual. The ICO approaches this issue in the following way: 'If you use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, you need to comply with Article 9.'[123] But there is a risk that such an approach is open to challenge. Article 9 of the UK GDPR requires the purpose of processing to be for 'unique identification'. Therefore, when biometric data is processed for another purpose, such as profiling an individual, it may be argued that this does not fall within the Article 9 UK GDPR conditions.

123 ICO. 'What is Special Category Data?'. *Guide to the General Data Protection Regulation (GDPR)*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

8.15 We consider this uncertainty to be a potential weakness in the current regime, notwithstanding the ICO's helpful attempt to clarify it. Data that has the capacity to uniquely identify an individual with some confidence is, at present, subject to lesser legal safeguards if it is being used for purposes other than unique identification.

8.16 Few witnesses had given consideration to the issues that could arise from the use of biometric data for classification or profiling purposes – though where they had, they recognised that those practices could be significantly rights-intrusive and needed careful regulation too.

8.17 The capacity of data to uniquely identify is an important defining characteristic of biometric data. We therefore do not consider that the current definition of biometric data under UK GDPR needs to be changed. While unique identification is potentially the most rights-intrusive use of biometrics, significant detriment may also be caused by the use of biometrics for categorisation or profiling purposes. There is an uncomfortable parallel with erroneous views by lawmakers that because the acquisition of the content of communications is potentially more intrusive than the acquisition of the metadata of communications, the latter needed far less protection.[124] That type of legislative wrong turn[125] is one that needs to be avoided in relation to the processing of biometric data for categorisation rather than identification.

8.18 The European Data Protection Board and European Data Protection Supervisor has deemed biometric categorisation to be sufficiently rights-intrusive to warrant a ban in circumstances where categorisation is undertaken on the basis of protected characteristics.[126] We did not receive sufficient evidence on this point to adopt the call for a ban. However, for the reasons below, we do believe that future regulation of biometric data should embed equal safeguards for biometric categorisation systems as biometric identification systems.

124 See *Big Brother Watch and others v UK* (Grand Chamber) App No.s 58170/13; 62322/14, 24960/15 at paragraph 364.
125 Regulation of Investigatory Powers Act 2000, Sections 15 and 16.
126 EDPS and EDPB, Joint Opinion, paragraph 33.

8.19 A new legal framework should seek to regulate this use of biometrics for categorisation with clarity. This would also allow new provisions to address discrimination issues that arise when biometric data is processed for purposes other than unique identification. But if biometric data is extracted from an individual, and then used for purposes other than individuation, statute must regulate the steps that a user must comply with, and the safeguards that must attach, to any other use of that data.

8.20 Indeed, the potential practical uses of biometric profiling or classification in everyday life are pertinent to the need to provide for safeguards in the new statutory scheme. Biometric classification may be readily deployable in a wide array of circumstances that would impact on individual liberties, for example, to ascertain eligibility for certain rights and services, including sifting through job applications or determining health status prior to travel. A recent EU-funded development of a border control system called iBorderCtrl deployed biometric classification 'to detect deception based on facial recognition technology and the measurement of, termed "biomarkers of deceit"'.[127] The ways in which such classifications could materially impact on individuals' lives – and the need for them to be clearly regulated – are self-evident.

8.21 This includes using biometric tools to classify individuals on the basis of characteristics that are protected by the Equality Act, potentially leading to discrimination. The Centre for Data Ethics and Innovation (CDEI) has raised concerns about algorithmic profiling around the use of Origins software by various police forces in the UK to determine whether particular ethnic groups specialise in particular types of crime.[128] The Ada Lovelace Institute has pointed out that such categorisations are particularly problematic if those using the tools are 'resorting to legal or scientific definitions that are in themselves contested, flawed or constructed in the context of a biased system and may overlook new axes of discrimination that can

127 Sánchez-Monedero, J.and Dencik, L. (2020). 'The politics of deceptive borders: "biomarkers of deceit" and the case of iBorderCtrl'. *Information, Communication & Society*,p.1. DOI: 10.1080/1369118X.2020.1792530

128 Centre for Data Ethics and Innovation (CDEI). (2020). *Review into bias in Algorithmic decision-making.* Available at: https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making

occur in algorithmic systems'. [129]

8.22 All of these factors lead us to conclude that any new legal framework should regulate the use of biometric data for identification and classification. It should not exclude the possibility of further regulation being necessary for other forms of processing if similar privacy rights infringements may arise.

Recommendation 3: Specific codes of practice on the use of biometric data should be published to regulate particular sectors and/or technologies. A compliance mechanism, similar to that given to the Scottish Biometrics Commissioner, should accompany such codes.

8.23 The extent to which new legislation can regulate the detail of how different types of biometric technology are used is limited. While legislation can and should set out the overarching framework, several witnesses emphasised that more fast-moving and granular detailed guidance will be necessary to ensure operational decisions about the use of biometrics are taken lawfully.

8.24 Codes of practice can fulfil that role and provide guidance the issues arising from specific uses of biometric data.

8.25 It is, of course, a precursor to proposing new codes of practice that there must be clarity as to which oversight body has primary responsibility for issuing such codes and what powers they have to do so. There must be consistency in the way guidance is given. This is something a new legal framework must address (See Recommendation 1 above). In relation to LFR, the numerous guidance documents issued by the ICO, the Surveillance Camera Commissioner and police – both at national and local level – illustrate the dangers of a fragmented approach. We have considered this further, below, under Recommendation 9.

129 Ada Lovelace Institute and DataKind UK. (2020). *Examining the Black Box: Tools for assessing algorithmic systems.* Available at: https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/

8.26 The detail of regulation of biometric technologies will differ between these uses and distinct codes of practice will be required. It is not possible to anticipate the range of uses of biometric data that will require regulation, and therefore focused consideration, rather than being covered by general legislation. For example, multimodal systems (which combine more than one type of biometric in a single system) are currently used in the US-VISIT programme, which uses the face and fingerprints, and in the Indian national identity AADHAAR card, which uses the face, iris and fingerprints. These variations may be best covered by codes of practice relating to use cases, rather than the technology being used.

8.27 Further distinct issues are raised by the development of behavioural biometrics such as gait and voice analysis or automated speech recognition (ASR). A recent paper indicated that significant racial disparities exist in the performance of five popular commercial ASR systems,[130] and each technology is likely to present its own challenges, which would need consideration in any appropriate code of practice.

8.28 It is not possible to set out in the abstract, what the content of any of the envisaged codes of practice should be. However, they should impose clear, accessible, and meaningful standards against which deployments of biometric technologies can be assessed and reviewed.

8.29 The processes and thresholds adopted by the codes of practice (for example, a requirement to fulfil specific criteria of reliability before being used; or how proportionality should be assessed) should be clearly defined. The codes of practice should enable public authorities and members to understand how decisions are made and what safeguards are in place.

8.30 An issue discussed at length during the course of our evidence sessions was the status that new codes of practice should have. Again, this is dependent on clarity as to which body should issue them and the statutory framework in which they are doing so.

130 Koenecke, A., Nam, A., Lake, E., Nudell, J., Quartey, M., Mengesha, Z. & Goel, S. (2020). 'Racial disparities in automated speech recognition'. *Proceedings of the National Academy of Sciences*, 7684-7689 117 (14). Available at: https://www.pnas.org/doi/10.1073/pnas.1915768117

8.31 Decision-makers will need to know whether they merely have to have regard to such codes, as opposed to being legally required to follow them. The latter approach has been adopted in Scotland, by way of Section 9(1) of the Scottish Biometrics Commissioner Act 2020. That provision states that police 'must comply' with the relevant code of practice. A breach of that obligation does not itself give rise to civil or criminal liability, but the Scottish Biometrics Commissioner can issue a compliance notice, failure to comply with which is a contempt of court.

8.32 Provided there is clarity as to who has responsibility for issuing relevant codes of practice within a new legal framework for the regulation of biometric data, we recommend that such codes should have a similar status for relevant stakeholders as the Code of Practice under the Scottish Biometrics Commissioner Act 2020. Relevant stakeholders should be required to comply to an applicable code of practice (though the codes may themselves provide for circumstances where departure from them may be permissible). A failure to comply with an applicable provision by a public authority would potentially be a public law error which could ground judicial review proceedings. But we also consider that a compliance regime (such as the compliance notice and contempt of court approach adopted in Scotland) should be part of the regulatory regime.

Recommendation 4: A legally binding code of practice governing LFR, and in particular the police use of LFR, should be published by the Government as soon as possible.

8.33 We agree with the recommendation in the ICO opinion of October 2019 that there should be a 'statutory and binding code of practice issued by Government'.[131]

8.34 LFR was the central concern of many of our witnesses. As the ICO's witnesses told us, there was a particular focus on it 'due to

131 ICO. (2019). *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places.* Available at: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

potential risks identified to data subjects', and taking account of its active use against the public. Current police use of LFR was the focus of that concern, though we also heard from witnesses concerned about public-private partnership uses (for example, the collaboration between the Metropolitan Police and Argent, a private company who own the King's Cross development area, to deploy facial recognition technology in the King's Cross area),[132] and purely private uses (for example, the use by Southern Co-op supermarkets of facial recognition technology in 18 of its stores).[133] LFR was described as a being carried out in a 'vacant regulatory landscape', with a 'responsive rather than proactive' model for regulation.[134]

8.35 Our LFR-specific recommendations respond to the predominance of LFR in the public consciousness and in the evidence that we received from stakeholders. It does not reflect any special status that we consider attaches inherently to LFR. Many other biometric technologies pose similar risks and challenges – but they are not in use or being developed to the same extent. As additional technologies or additional uses emerge, in our view the safeguards that we currently propose in respect of LFR are very likely to be necessary in other contexts, too.

8.36 The ruling by the Court of Appeal in the *Bridges* case commented that 'too much discretion is currently left to individual police officers' to decide the deployment and targets of LFR, with the Court recommending consistency at the national level.[135] The former Biometrics Commissioner welcomed moves by the Home Office that could deal with this deficiency by creating national guidelines for the use of facial matching by police in England & Wales. We were aware, from our evidence-taking, that the College of Policing was developing guidelines on LFR use and was consulting on a new code of practice on information management by the police generally. The College of Policing has now published

132 Sabbagh, D. (2019). 'Facial recognition row: police gave King's Cross owner images of seven people'. *The Guardian.* Available at: https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people

133 Wakefield, J. (2020). 'Co-op facial recognition trial raises privacy concerns'. *BBC News.* Available at: https://www.bbc.co.uk/news/technology-55259179

134 Evidence of Suzanne Shale.

135 *Bridges*, at paragraph 91.

authorised professional practice on police use of LFR.[136] We understand that the National Police Chiefs Council (NPCC) is also developing guidance on the creation and management of watchlists. We consider that these might provide a useful interim measure, but a statutory and centrally promulgated code of practice will ultimately be necessary to regulate this sensitive area. We are also concerned that some of those bodies seeking to publish their own guidance documents on LFR have differing views on fundamental issues, including the interpretation of the *Bridges* judgment.

8.37 If the ICO's recommendation for a single, Government-issued code of practice is taken up, it would clarify the limitations on the use of LFR, setting the required criteria for strict necessity and proportionality and required safeguards.

8.38 The ICO is also consulting on an auditing framework for AI, which would be applicable to LFR users and vendors.[137] A report by the Royal United Services Institute (RUSI) on the use of algorithms by police, commissioned by the CDEI, found the lack of national consistency guidance to be the biggest issue raised by the law enforcement community,[138] and proposed a new code for algorithmic tools in policing as the means to address this current inadequacy. For them, a new code should establish 'clear roles and responsibilities regarding scrutiny, regulation and enforcement' for the NPCC, Home Office, College of Policing and regulators such as the ICO and IPCO. This echoes some of the concerns we heard about the fragmentation of regulation in this area.

8.39 RUSI argues that a new code should also create 'a standard process for model design, development, trialling, and deployment, along with ongoing monitoring and evaluation. It should provide clear operationally relevant guidelines and complement existing authorised professional practice and

136 College of Policing. *Authorised Professional Practice: Live Facial Recognition*. Available at: https://www.app.college.police.uk/app-content/live-facial-recognition/?s=

137 ICO. (2020). *Guidance on the AI auditing framework: Draft guidance for consultatio*n. Available at: https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf

138 Babuta, A. and Oswald, M. (2020). 'Data Analytics and Algorithms in Policing in England and Wales: Towards A New Policy Framework'. *RUSI*. Available at: https://rusi.org/publication/occasional-papers/data-analytics-and-algorithms-policing-england-and-wales-towards-new

other guidance in a tech-agnostic way'.[139] We share and echo that view.

8.40 The College of Policing's new authorised professional practice (APP) on LFR, published in March 2022, is likely the most detailed guidance on LFR, at least in a policing context. The APP covers the legal framework following the *Bridges* decision and therefore provides wide-ranging discussion of, for example, the importance of the public sector equality duty. It also goes beyond strict legal requirements, and covers topics such as operational governance, as well as undertaking 'community impact assessments' and committing to ongoing community engagement.

8.41 However, as it is only authorised professional practice, police adherence is discretionary rather than mandatory. This undermines the APP's ability to ensure standardised practice across the regional police forces. It also lowers the guidance's ability to be used as a mechanism for enhancing accountability with police use of LFR. In our view, a code of practice that was binding on the police would ensure that these issues are addressed.

8.42 The former Surveillance Camera Commissioner made various recommendations for the Home Office and NPCC, ranging from introducing an authorisation process by a senior officer not involved in the operation, to improving guidance for human decision-making and national performance indicators. The College of Policing's LFR APP recommends that any deployment of LFR is authorised in writing by an authorising officer, not below the rank of superintendent, and that the authorising officer should be distinct from the officer with operational command over LFR deployment 'on the ground'. The creation of a 'standard trials methodology' to provide quality evidence base for future decisions is also recommended by the former Biometrics Commissioner,[140] who has also recommended improvements to Home Office data systems, including the Police National Database, to be able to implement privacy-by-design and legal compliance processes, such as the

139 Babuta, A. and Oswald, M. (2020).

140 Biometrics Commissioner. (2020). *Annual Report 2019*. Available at: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019

automatic deletion of biometric data.[141] We would suggest that these recommendations ought to be taken into account in the content of an LFR Code of Practice.

8.43 A new LFR code will also have to deal with public-private collaborations, which the College of Policing's APP expressly states is out of scope of the guidance. The subcontracting of facial recognition services and police access to privately assembled biometric datasets are the two most prominent issues in this regard. Permissive standards applied to private companies risk undermining the safeguards which exist, or which might be introduced, in respect of public authority use. This is because, without clear limitations being put in place, public authorities may access private companies' datasets and data tools through public-private partnerships. While such an agreement may be lawful,[142] that does not lessen the importance of providing further guidance for those who might wish to create such a partnership, and embed further safeguards for those who might be affected.

8.44 Indeed, there is nothing inherently less rights-intrusive about private use of LFR to which public authorities may have access and an LFR Code of Practice will need to grapple with these complexities.

8.45 One striking example of public use of private biometric data is the US company Clearview AI. It used more than three billion images scraped from millions of websites including Facebook and YouTube to create a facial recognition search engine. Their search engine was then used by over 600 law enforcement agencies and other organisations in the US without adequate safeguards or public scrutiny.[143] Investigative journalists found that several European police forces have also used Clearview. The Swedish data protection authority has fined a police authority for its use,[144] and the Hamburg Data Protection Authority has deemed such biometric profiles of people in the EU illegal and ordered the

141 Biometrics Commissioner. (2020)

142 See for example: *R (M) v Chief Constable of Sussex & anor*. [2021] EWCA Civ 42.

143 Hill, K. (2020). 'The Secretive Company That Might End Privacy as We Know It'. *The New York Times*. Available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

144 Lomas, N. (2021). 'Sweden's data watchdog slaps police for unlawful use of Clearview AI'.*Techcrunch*. Available at: https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/

company to delete the biometric profile of the person who raised a complaint.[145] *Buzzfeed News* reported that the Metropolitan Police and the National Crime Agency, along with 'a number of other police forces, private investment firms, the Ministry of Defence...' had carried out hundreds of searches using the service.[146] The ICO opened an investigation into the personal information handling practices of Clearview AI, which concluded with the ICO announcing its provisional intent to impose a fine of slightly over £17 million on the company.[147]

8.46 As the former Biometrics Commissioner confirmed in his evidence to us, 'the boundary between public policing and private policing has been blurred by biometric technology', and the former Surveillance Camera Commissioner recommended the regulation of police engagement with the private sector. While we accept (see Recommendation 10, below) that further work needs to be done on the regulation of biometrics in the private sphere, it is quite clear that for a code of practice to properly regulate the ongoing and present issues arising from LFR, it must provide for regulation of public-private collaboration and for safeguards in relation to private-sector use as well. We note and endorse the factors identified by the Biometrics and Forensics Ethics Group in its briefing note on the ethical issues arising from public-private collaboration in the use of LFR technology[148] and the standards that ought to be imposed by a code of practice before such collaboration is permissible: the user to demonstrate that (1) the collaboration is necessary, (2) that the data-sharing required by the collaboration is proportionate and (3) that there is clarity in the types of data that will be shared.

145 Noyb.(2021). 'Clearview AI deemed illegal in the EU, but only partial deletion ordered'. *noyb.eu*. Available at: https://noyb.eu/en/clearview-ai-deemed-illegal-eu

146 Ashton, E. and Mac, R. (2020). 'More Than A Dozen Organizations From The Met Police To J.K. Rowling's Foundation Have Tried Clearview AI's Facial Recognition Tech'. *Buzzfeed*. Available at: https://www.buzzfeed.com/emilyashton/clearview-users-police-uk

147 ICO. (2021). *ICO issues provisional view to fine Clearview AI Inc over £17 million*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/

148 BFEG. (2021). *Briefing note on the ethical issues arising from public– private collaboration in the use of live facial recognition technology*. Available at: https://www.gov.uk/government/publications/public-private-use-of-live-facial-recognition-technology-ethical-issues/briefing-note-on-the-ethical-issues-arising-from-public-private-collaboration-in-the-use-of-live-facial-recognition-technology-accessible

Recommendation 5: The use of LFR in any circumstance should be suspended until a new statutory framework and code of practice are in place

8.47 The reliance by police on common-law powers to carry out live facial recognition and potentially other intrusive biometric surveillance has been criticised by Daragh Murray and Peter Fussey, who have studied police deployments of LFR. In their view it is inconsistent with the UK's obligations under the Human Rights Act and European Convention on Human Rights and they suggest that, 'establishing an explicit legal and regulatory basis for the use of LFR would provide much needed clarity, both for the public and for the police.'[149] While the Court of Appeal in *Bridges* found that the common law provided the source of the police's power to use LFR technology, it found at the same time that the manner in which that power was used (without an adequate legal framework) violated individual privacy rights. It was of significant concern to us that this was not always clearly understood by those working with guidance and devising policy in this area.

8.48 Due to the concerns raised about the rights-intrusion caused by LFR, many organisations and campaigning groups have called for an outright ban on live facial recognition in public places and/or a moratorium or the ban of specific uses. Human rights groups Liberty, Big Brother Watch and Privacy International are all campaigning to stop facial recognition. In their evidence to the Review, Liberty and Big Brother Watch confirmed that their organisations seek a total ban on LFR. A large coalition of European rights groups launched a public campaign to get 1 million signatures to 'ban biometric mass surveillance' in public spaces within the EU.[150] The German think tank AlgorithmWatch has found that 'public uses of facial recognition that might amount to mass surveillance are decisively banned until further notice, and urgently, at the EU level'.[151] Local bans on LFR have been issued by

149 Fussey, P. and Murray, D. (2020). 'Policing Uses of Live Facial Recognition in the United Kingdom' in Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions.* AI Now Institute. Available at: https://ainowinstitute.org/regulatingbiometrics.html

150 See: https://reclaimyourface.eu/

151 Chiusi, F., Fischer, S., Kayser-Bril, N. and Spielkamp, M. (eds.). (2020). *Automating Society Report 2020*. AlgorithmWatch. Available at: https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf

municipalities in the US, starting in San Francisco, following local campaigns from citizens and rights organisations. In the summer of 2020, several technology companies were driven by the public protests about racism and policing in the US and elsewhere to introduce unilateral moratoria on facial recognition. IBM was the first to announce that it would not offer general purpose facial recognition or analysis software, asking for a 'national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies'.[152] Soon after, Amazon announced a one-year moratorium on police use of their facial recognition technology Rekognition, while still allowing its use by organisations working to rescue human trafficking victims and reunite missing children with their families.[153] It is worth noting that the ACLU was quick to point out that they had already asked Amazon in 2018 to stop providing this technology to governments[154] and demanded a 'blanket moratorium on law enforcement use of facial recognition until the dangers can be fully addressed'.

8.49 The UK group WebrootsUK has called for a 'generational moratorium' of several decades on LFR, which they position 'between a moratorium and a general ban'. They view that long time span as necessary for addressing 'the much deeper societal issues related to racialised surveillance', while recognising 'that the technology could have a role to play in an anti-racist society for specific purposes, e.g. identifying missing children'.[155]

8.50 We consider the numerous and varied voices calling for a ban on LFR – from a diverse range of stakeholders – to be persuasive. We are fortified in that view by the key legal challenge to LFR in England finding it to be unlawful. For that reason we recommend a complete moratorium on the use of LFR by public and private entities until a sufficient legal framework in place.

152 IBM. (2020). 'IBM CEO's Letter to Congress on Racial Justice Reform'. *IBM Policy Lab*. Available at: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/

153 Amazon. (2020). 'We are implementing a one-year moratorium on police use of Rekognition'. *aboutAmazon.com*. Available at: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

154 American Civil Liberties Union (ACLU). (2018). *Letter from Nationwide Coalition to Amazon CEO Jeff Bezos regarding Rekognition*. Available at: https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition

155 Chowdhury, A. (2020). 'Unmasking Facial Recognition: An exploration of the racial bias implications of facial recognition surveillance in the United Kingdom'. *WebRoots Democracy*. Available at: https://webrootsdemocracy.files.wordpress.com/2020/08/unmasking-facial-recognition-webroots-democracy.pdf

8.51 We do not believe this is a radical position: it is supported by the organisations cited above, among others, and there is precedent for it. AI Now has called for a halt to all use of facial recognition in sensitive social and political contexts until the risks are fully studied and adequate regulations are in place.[156] Microsoft have said they will not sell facial recognition technology to US police forces until a federal law is passed.[157] The US Senate has introduced a bill for a Facial Recognition and Biometric Technology Moratorium Act prohibiting federal use of certain biometric technologies.[158] In the UK, The House of Commons Science and Technology Committee has said that 'facial recognition technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved', asking for Parliament to have 'an opportunity to debate and vote on the issue'.[159] We strongly endorse this position, and would go further: even piloting should cease until a proper legal framework is in place. The deployment analysed by the courts in *Bridges* were 'pilots' but that did not prevent them from violating individual rights.

8.52 We do not, however, go as far as the human rights organisations who call for a permanent ban on the use of LFR. With a proper legal framework, we cannot exclude the possibility that it could be deployed in a rights-compatible way. But, we are persuaded that, at present, it is not possible. We therefore recommend a moratorium on its use until an adequate legal framework is introduced.

156 AI Now. (2019). *AI Now 2019 Report*. Available at: https://ainowinstitute.org/AI_Now_2019_Report.pdf

157 Greene, J. (2020). 'Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM'. *The Washington Post*. Available at: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/

158 Facial Recognition and Biometric Technology Moratorium Act, S.4084, 116th Cong. (2020) <https://www.congress.gov/bill/116th-congress/senate-bill/4084>.

159 House of Commons Science and Technology Committee. (2018). *Biometrics strategy and forensic services: Fifth Report of Session 2017–19*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/800/800.pdf

Recommendation 6: Duties arising under the Human Rights Act 1998, Equality Act 2010 and Data Protection Act 2018 should continue to apply to uses of biometric data

8.53 In our view, the need for new legislation and codes of practice focused on biometric data is because of current gaps in the legal framework to properly regulate the use of these technologies. We do not, however, consider that the more general legal framework should no longer apply in the context of biometrics – there are important legal duties under the Human Rights Act, UK GDPR, DPA 2018 and Equality Act which will and must continue to apply to uses of biometrics. The existing duties are not sufficient but they remain, in our view, necessary.

8.54 The most important existing duties are: (1) the obligation on public authorities not to violate rights protected by the Human Rights Act; (2) the obligation not to discriminate, directly or indirectly, and (for public authorities) to comply with the public sector equality duty;[160] and (3) data processing obligations.

8.55 In evidence to the Review, the CDEI noted that 'organisations struggle to interpret the law', and we recommend that the biometrics statutory framework incorporates, clarifies and augments the existing duties to provide a clear and logical framework which users must follow before any potential use of biometrics can occur.

8.56 Many of the principles that we consider should form the basis of a new legislation find their origin in human rights and data protection law. Necessity, for example, is a crucial duty under both regimes. According to the European Data Protection Supervisor (EDPS), processing of biometric data for uniquely identifying purposes cannot take place unless one can rely on specific exemptions for special category data in GDPR, also found in the new UK GDPR.[161] Its use must be demonstrably necessary, meaning that there are no other less intrusive means.

160 See our discussion of what the PSED requires in this context, at paragraph 5.37. above.

161 Wiewiórowski, W. (2019). 'Facial recognition: A solution in search of a problem?'. *European Data Protection Supervisor*. Available at: https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en

8.57 The EDPS identifies as particular data protection problems the impossibility of claiming consent in the monitoring of public spaces and the difficulties with implementing data minimisation and a privacy-by-design approach, as required by law.[162] The problems with ineffective consent have also been raised in the US context, where laws such as the Illinois Biometric Privacy Act (BIPA) force businesses to ask for consent before collecting biometrics data.[163]

8.58 There is consensus on the need for impact assessments both under data protection and equality legislation. The former Surveillance Camera Commissioner recommended that 'the Home Office, regulators and other stakeholders collaborate to consider the development of a single "integrated impact assessment" process/format which provides for a comprehensive approach to such matters. This is to improve focus, reduce duplication, reduce bureaucracy and avoid gaps'.[164]

8.59 While our proposal is for those impact assessments to remain standalone, we agree with the Surveillance Camera Commissioner that both are crucial and should be incorporated as prior obligations under the Biometrics Bill.

Recommendation 7: A national Biometrics Ethics Board should be established, and given a mandatory advisory role in respect of public-sector biometrics use

8.60 One of our key concerns, discussed extensively with various witnesses to the Review, was the absence – at present – of any formal process for ethics to be taken into account in respect of operational decisions relating to biometric technologies.

8.61 While the Biometric and Forensics Ethics Group (BFEG) has

162 Wiewiórowski, W. (2019).

163 Hartzog, W. (2020). 'BIPA: The Most Important Biometric Privacy Law in the US?' in Kak, A. (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute. Available at: https://ainowinstitute.org/regulatingbiometrics.html

164 Surveillance Camera Commissioner. (2020). *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*, paragraph 3.86. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

produced some impressive and thoughtful papers on the ethical implications of various biometrics uses, their role is limited to advising the Home Office and we found that witnesses were not well-acquainted with their work.

8.62 West Midlands Police and the Metropolitan Police have established their own ethics processes but they are exceptions. Most police forces do not have ethics boards and there is no formal provision for ethical oversight of any other public bodies which may use biometrics. This is unsatisfactory. Ethical considerations are critical: as Detective Chief Superindendent Chris Todd of West Midlands Police observed, 'in order to maintain legitimacy, ethics must be embedded' alongside the law. Suzanne Shale, Chair of the London Policing Ethics Panel, told us that until recently 'it was striking to see how little ethical scrutiny there was of trials of policing technologies of the population'.[165] The witnesses working in law enforcement generally agreed that 'the concept of a national ethics body is a good thing.'[166]

8.63 Suzanne Shale underscored the benefits that can accrue from external ethical oversight, independent from the operational decision-making structure – though several witnesses also warned of the risk that externalising ethical considerations may allow organisations to ignore ethics internally. We accept the existence of that risk, but we consider that external, ethical oversight is necessary in a field as complex and sensitive as biometrics, and that the formalising of ethical oversight can play a positive role in emphasising the importance of, and therefore embedding, ethical principles in decision-making around biometrics.

8.64 Supportive of our view that a national Biometrics Ethics Board should be established, the CDEI in a review found that correcting the fragmentation of responsibility for the ethical use of data in the policing context requires leadership from the Home Office to define roles and responsibilities and ensure that 'work underway by the National Police Chiefs' Council and other policing stakeholders to develop guidance and ensure ethical oversight of data analytics tools is appropriately

165 Evidence of Suzanne Shale.
166 Evidence of the College of Policing.

supported'[167]. For the CDEI, there is a need to 'establish standard processes for independent ethical review and oversight to ensure transparency and accountability and facilitate meaningful public engagement before tools are deployed operationally'.

8.65 The former Surveillance Camera Commissioner has also recommended that police use of LFR is subjected to meaningful and independent ethical oversight from the initial planning to before and during operations. He supports Ethics Committees, or in their absence a multiagency structure similar to that created for stop and search.[168] Taking account of both *Bridges*, and the views expressed by the witnesses with whom we spoke, we recommend that a single, independent national Biometrics Ethics Board should be established to provide ethical oversight.

8.66 The good practice of BFEG, the London Policing Ethics Panel, and the West Midlands Police ethics committee should all inform the establishment, and membership, of this Board. We have considered the example of the national DNA and fingerprints database, which is overseen by the Forensic Information Databases Strategy Board (FIND-SB), and which includes representatives of the NPCC, Home Office and Police and Crime Commissioners.[169] We consider that greater independence is necessary in our proposed Biometrics Ethics Board: parties with a stake in operational decision-making should not be members of the Board, although those with experience of law enforcement (for example, retired Chief Constables) are likely to have a valuable role to play. Otherwise, the Board should be comprised of a mix of members with expertise in ethics, human rights and relevant technology.

167 CDEI. (2020). *Review into bias in algorithmic decision-making*. Available at : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

168 Surveillance Camera Commissioner. (2020). *Facing the Camera: Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*, paragraph 2.26. Available at : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf

169 Biometrics Commissioner. (2020). *Annual Report 2019*, chapter 4. Available at: https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019

Recommendation 8: The Biometrics Ethics Board's advice should be published. Where a decision is taken to deploy biometric technology contrary to the advice of the Ethics Board, the deploying body should publish, within 14 days of the Ethics Board's advice, a summary explanation of their reasons for rejecting the Board's advice, or the steps they have taken to respond to the Board's advice prior to deployment.

8.67 Although there was broad support among our witnesses for the establishment of a national Biometrics Ethics Board, there were divergent views on the extent of powers that it should be given. There was general agreement that 'the role of the Ethics Committee should be to expose or highlight concerns'[170], but those working in law enforcement believed that autonomy of operational decision-making by the police remained crucial. In their view an Ethics Board that did not have the power to veto deployments and could only consider matters referred to it by the police would be 'in the right place on the spectrum'.[171] Part of the rationale given for its being a referral-by-choice system was that 'there wouldn't be a scenario where [the police] wouldn't want to subject' important issues to scrutiny.[172]

8.68 In our view, it is right that the Ethics Board should not have the power to veto deployments, and that the ultimate decision-making on whether to proceed with a particular use of biometric technology should rest with operational decision-makers. We do not, however, agree that a referral-by-choice system would be sufficiently robust (and we put to all witnesses who suggested it that if they were right that public bodies would always want ethical input, there would be no detriment in such input being mandatory). We recognise that there may be exceptional circumstances in which referral to an Ethics Board may not be possible before a particular deployment, for reasons of urgency or sensitivity. But those occasions will be very limited, and in general we consider that

170 Evidence of the College of Policing.
171 Evidence of Chris Todd.
172 Evidence of Lindsey Chiswick.

every proposed use by a public body of biometric technologies on members of the public should be subject to mandatory referral to a national Ethics Board.

8.69 We also recommend that the advice of the Ethics Board is published and that a public authority choosing to deploy the use of biometric technology against the advice of the Ethics Board should be required to publish reasons justifying its position. Those steps will protect transparency and accountability and encourage public confidence and credibility in the process. We agree that 'the design and implementation process should be as transparent and as open to public scrutiny as possible.'[173] Public consideration by an Ethics Board will be one means of achieving this.

8.70 It will be for others to determine when and how quickly such reasons should be published, but we see no reason why – subject to narrow and justifiable exceptions – the reasons should not be published within 14 days of the decision to reject the Ethics Board recommendation and prior to the deployment commencing.

8.71 The publication of advice will also provide the public with an understanding of the issues and risks identified in respect of different intended uses, and will equip them with the knowledge necessary to challenge any problematic uses. That is a critical aspect of democratic legitimacy and accountability. As the German Data Ethics Commission has stressed:

'It is vitally important to ensure not only that the users of algorithmic systems understand how these systems function and can explain and control them, but also that the parties affected by a decision are provided with sufficient information to exercise their rights properly and challenge the decision if necessary.'[174]

8.72 The House of Commons Science and Technology Committee (STC), heard in evidence from the ICO that ethics boards can

173 Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*. The Alan Turing Institute. Available at: https://doi.org/10.5281/zenodo.3240529

174 German Federal Government's Data Ethics Commission. (2019). *Opinion of the Data Ethics Commission*. Available at: https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.htm

aid transparency by publishing their deliberations, so that the development of the algorithm is openly documented. The STC recommended that where there is a conflict with commercial confidentiality or privacy, the CDEI should help with improving the transparency and explainability of the system.[175]

8.73 The CDEI has set a clear priority for transparency in algorithmic systems, which would include biometrics and facial recognition:

'Government should place a mandatory transparency obligation on all public sector organisations using algorithms that have a significant influence on significant decisions affecting individuals... it should require the proactive publication of information on how the decision to use an algorithm was made, the type of algorithm, how it is used in the overall decision-making process, and steps taken to ensure fair treatment of individuals.'[176]

8.74 Our recommendation that the advice of the Ethics Board – and any response from the public body – be published is reflective of and consistent with these views.

Recommendation 9: Oversight functions should be consolidated, clarified and properly resourced.

8.75 The effectiveness of our recommendations also requires oversight functions over biometric data should be consolidated, clarified and properly resourced.

8.76 We accept that such consolidation and clarity may be achieved by strengthening the ICO's capacity in regard to biometrics. But we believe that the prominence and importance of biometrics means that it requires a specialist Commissioner. We note, in particular, the powerful points advanced by the current Biometrics and Surveillance Camera Commissioner against his role being

175 House of Commons Science and Technology Committee. (2018). *Algorithms in decision-making*. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/35102.htm

176 CDEI. (2020). *Review into bias in Algorithmic decision-making.* Available at: https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making

incorporated into the work of the ICO, in his blogpost *What we talk about when we talk about biometrics....* [177]

8.77 Wherever that role is located, it must be adequately resourced financially, and have both sufficient powers and expertise to perform the governance that a role like this requires.

8.78 Many of the witnesses believed that regulatory simplicity would be desirable, and that the current oversight structures were unduly complex and fragmented. The current regulatory landscape was characterised as one of 'regulatory overlaps', which is 'confusing'.

8.79 However, those same witnesses had highly conflicting views as to which existing or hypothetical regulators should take the reigns over the various uses of biometric technologies. The former Surveillance Camera Commissioner, like his successor, argued that maintaining a specialist Commissioner 'provides for democratic engagement and accountability', while the ICO considered that biometrics oversight was an area that could probably be accomplished by them within their existing remit. Others noted that as personal data and technology becomes more and more central to the way in which society operates, there is a risk of overloading the ICO with too broad a role in too many areas. There is a danger of it becoming a behemoth responsible for regulating all aspects of life without the capacity to address any particular area in the detail, or with the resources necessary. There would be a risk that a Commissioner located in the ICO, under the Information Commissioner, would be less accessible to the public and less accountable than a standalone role.

8.80 We note the views on both sides about this. We consider that biometrics are sufficiently prominent as a cause of concern and emerging opportunity and risk in society that a named, prominent Commissioner is necessary. In our view, that could be achieved in various formats, and we do not recommend any particular 'location' of the role over any other. We note that, if a standalone Commissioner role is created or strengthened (perhaps by an evolution of the now-consolidated Biometrics and Surveillance

177 Biometrics and Surveillance Camera Commissioner. (2021). *What we talk about when we talk about biometrics...*. Available at https://videosurveillance.blog.gov.uk/2021/10/12/what-we-talk-about-when-we-talk-about-biometrics/

Camera Commissioner role), the ICO would still continue to play a role in the regulatory oversight of biometrics: UK GDPR makes the Information Commissioner the sole supervisory authority for data protection purposes,[178] including to handle complaints and enforce data protection compliance. If a Commissioner role is created outside the ICO, there would need to be clear processes for the referral of complaints or enforcement requests between the two bodies.

8.81 Wherever it sits, there are certain features that the regulator must have: primarily, adequate resourcing, expertise, powers and capacities. For example:

1. The Competition and Markets Authority (CMA) has stipulated that a regulator of AI systems must have the capacity to perform continuous monitoring of biometric systems: one-off audits may become quickly outdated, so ongoing monitoring is therefore necessary.[179] We agree.

2. The regulator must also be technically capable and legally empowered to carry out a variety of assessments.[180] Linked to the discussions on transparency in the previous section, the regulator needs to be able to check for bias in outcomes and the overall compliance of the systems with the applicable regulations.

3. The regulator must have appropriate equality expertise; as the CDEI has pointed out, 'the PSED (public sector equality duty) also extends to regulators who are responsible, as public sector bodies, to ensure the industry they regulate is upholding appropriate standards for testing for bias in the use of algorithms. In order for regulators to fulfil these obligations, they will need support, through building relationships between regulators and from organisations with specific expertise in

178 General Data Protection Regulation Keeling Schedule showing changes which would be affected by the Data Protection, Privacy And Electronic Communications (Amendments Etc)(EU Exit) Regulations 2019 MADE ON 28 FEBRUARY 2019 (As amended by the Data Protection, Privacy And Electronic Communications (Amendments Etc)(EU Exit) Regulations 2020 laid on 14 October 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969514/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V4.pdf>

179 Competition and Markets Authority. (2021). *Algorithms: How they can reduce competition and harm consumers*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954331/Algorithms_++.pdf

180 Ada Lovelace Institute and DataKind. (2020). *Examining the Black Box*. Available at: https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/

these areas.'[181] That is, of course, of particular importance in the field of biometrics where the risk of discrimination is so acute.

Recommendation 10: Further work is necessary on the topic of private-sector use of biometrics and public/private sharing of biometrics.

8.82 Despite our early aspirations, we have not been able to investigate and reach conclusions on the regulation of private-sector uses of biometrics to the extent that we would have liked. That the focus in our Review is on public-sector, and particularly police, uses of biometrics should not be interpreted as an acceptance that those are the most important or sensitive uses of biometrics, requiring the greatest safeguards. As the CDEI captured the point succinctly: 'The potential for nefarious use in the private sector is as present as it is in the public sector.'

8.83 We did not, however, receive engagement from private-sector stakeholders to the same extent as from public authorities; the witnesses with whom we spoke were less knowledgeable on private-sector issues than public-sector issues; and the literature on private-sector uses of biometrics is less well developed. As a consequence, our final recommendation is that further work is commissioned that focuses specifically on private-sector use and the particular concerns and requirements for regulation that arise in that sphere.

8.84 There are two particular areas of private-sector use that appeared, to us, in the course of conducting the Review, to warrant particular attention. The first, as addressed earlier, is the issue of public-private collaboration. The second is the use of biometrics in the workplace.

8.85 The issue of public-private collaboration came to particular prominence in the summer of 2019, when the Financial Times reported that the managers of the King's Cross estate in London,

181 Ahamat, G. (2020). *Public Sector Equality Duty and bias in algorithms*. CDEI. Available at: https://cdei.blog.gov.uk/2020/12/09/public-sector-equality-duty-and-bias-in-algorithms/

a large private property development, had been using facial recognition for two years to track thousands of people.[182] After initial denials it transpired that the Metropolitan Police and British Transport Police had given the company databases of persons of interest.[183] The estate managers claimed that the system was used to help the police in fighting crime in the area and that all data had been deleted.[184] Other LFR partnerships between police and private sector operators have been reported in Manchester,[185] where a single positive match was made out of 15 million samples, and in Sheffield.[186] The ICO started an investigation on the King's Cross incident in August 2019[187] but has not, to date, published any findings.

8.86 The scale of public-private collaboration on LFR could grow dramatically if plans for an updated 'ring of steel' in the City of London come to fruition. The City built a CCTV security perimeter barrier after the IRA bombings in the 1990s, through which police can take control over privately owned cameras. City of London Police wants to upgrade their pioneering but now outdated CCTV system, with a central control room and links to 'smart' city technology such as street lighting. The force also wants to integrate LFR in the new system.[188]

8.87 Other recent private users of LFR include Southern Co-op supermarkets, where 18 shops have been using the facial recognition technology to reduce shoplifting and abuse against staff.[189] The system used, by a company called Facewatch,

182 Madhumita Murgia, M. (2019). 'London's King's Cross uses facial recognition in security cameras'. *Financial Times*. Available at: https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c

183 The London Assembly, Questions to the Mayor (MQT on 2019-07-18) <https://www.london.gov.uk/questions/2019/14214#a-173736>

184 King's Cross Central Limited Partnership (KCCLP). (2019). *Updated Statement: Facial Recognition*. Available at: https://www.kingscross.co.uk/press/2019/09/02/facial-recognition

185 Robson, S. (2018) 'Trafford Centre bosses explain why they used controversial cameras to monitor shoppers'. *Manchester Evening News*. Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/trafford-centre-bosses-explain-used-15283677

186 BBC Sheffield & South Yorkshire. (2019). 'Meadowhall shoppers scanned in facial recognition trial'. Available at: https://www.bbc.co.uk/news/uk-england-south-yorkshire-49369772

187 ICO. (2019). *Statement: Live facial recognition technology in King's Cross*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

188 Professional Security Magazine. (2018). 'New "ring of steel" proposed'. Available at: https://www.professionalsecurity.co.uk/news/interviews/new-ring-of-steel-proposed/

189 Burgess, M. (2020). 'Co-op is using facial recognition tech to scan and track shoppers'. *Wired UK*. Available at: https://www.wired.co.uk/article/coop-facial-recognition#:~:text=Branches%20of%20Co%2Dop%20in,shoplifting%20and%20abuse%20against%20staff

compiles watchlists from the individuals flagged by their various clients. The lack of any safeguards over the creation of watchlists in the private sector raises particular equality and discrimination concerns. Similar developments have taken place elsewhere: in the US, the pharmacy chain Rite Aid installed facial recognition systems in hundreds of stores over a period of eight years. Most deployments were in low-income non-white areas. The practice stopped in 2020 after an in-depth investigation by Reuters.[190]

8.88 As the Biometrics and Forensics Ethics Group found in its report on public-private collaboration in LFR, real-time collaborative deployment of LFR technology means that it is not just images that are shared by collaborators, but a wider biometric data system that can be combined and processed with other data sources: 'machine learning tools, deep neural network algorithms, training datasets, and so on. For example, the providers of the LFR technology could use data collected during [public-private] collaborations to train or refine their algorithm... (This) means that datasets collected for one purpose (and by one organisation) are repurposed for processing in a new way by another organisation, which has implications for the data subjects' rights'. This is a particular issue with the use of cloud-based platforms that enable data from various sources to be used in machine-learning 'without any actual "sharing"'.

8.89 These concerns are only likely to increase as private uses of biometric technology proliferate. While we have recommended that new legislation should ensure that obligations on private entities using biometric data should be similar to those imposed on public authorities, we recommend that further work is undertaken to ascertain the specific additional safeguards and duties that may be necessary to ensure adequate regulation of private-sector, and private-public collaboration, uses of biometrics.

8.90 The other key area of concern in the private sector is the use of biometrics in the workplace. This came became particularly noticeable as the Review was conducted over the course of the COVID-19 pandemic. The shift to remote working and videoconferencing accelerated by the pandemic means that many

190 Dastin, J. (2020). 'Rite Aid deployed facial recognition systems in hundreds of U.S. stores'. *Reuters Investigates*. Available at: https://www.reuters.com/investigates/special-report/usa-riteaid-software/

interactions are now digital, which enables forms of processing that are not possible in face-to-face communications. Over a quarter of large firms surveyed said they had implemented remote monitoring or planned to do so.[191] This may cause existing deployments of AI and analytics to proliferate, building on technologies that are already in place, for example, in call centres – such as speech analytics, text analytics, sentiment analysis, customer behaviour prediction, persona-based interactions, presented as a way to enable more 'meaningful conversations'[192] at a distance.

8.91 One example of workplace monitoring is the development by PwC of a facial recognition tool to check whether remote workers left their screens. The tool was developed for financial firms with strict compliance requirements, presumably to avoid information leaks or backroom deals during the pandemic, but it raised concerns about its intrusiveness and its potential to be used by employers for other purposes.[193]

8.92 The trade union Prospect found that 80% of polled workers were uncomfortable with camera monitoring and similarly high proportions were also opposed to other forms of monitoring such as keystroke recording.[194] UNISON has published a guide on monitoring and surveillance at work,[195] which notes that UNISON members have seen an increase in the use of biometrics for staff time-keeping and sickness absence. A recent report by the TUC on the impact of technology in the workplace found that biometrics were still experienced by only a small proportion of workers, but identified as a key objective achieving more worker consultation on the development, introduction and operation of new technologies in the workplace.[196]

191 Dodd, V. (2020). 'Remote-working Compliance YouGov Survey'. *Skillcast*. Available at: https://www.skillcast.com/blog/remote-working-compliance-survey-key-findings

192 Dharshan, N., Nair, P., Nagraj, B. and Aase, J.E. (2020). 'ISG Provider Lens™ Contact Center - Customer Experience Services - Global 2020.' ISG Research. Available at:https://research.isg-one.com/reportaction/Quadrant-CC-Global-2020/Marketing

193 McNulty, L. and Kelley, T. (2020). 'PwC under fire for tech that tracks traders' loo breaks'. *Financial News*. Available at: https://www.fnlondon.com/articles/pwc-under-fire-for-tech-that-tracks-traders-loo-breaks-20200615

194 Prospect. (2020). *Workers are not prepared for the future of working from home*. Available at: https://prospect.org.uk/news/workers-are-not-prepared-for-the-future-of-working-from-home/

195 UNISON. (2020). *Bargaining On Monitoring And Surveillance Workplace Policies*. Available at: https://www.unison.org.uk/content/uploads/2018/08/Monitoring-and-surveillance-at-work-08-2018.pdf

196 Trade Union Congress (TUC). (2020). *Technology Managing People - the worker experience*. Available at: https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf

8.93 A report on AI and discrimination by Robin Allen QC and Dee Masters found that, among other things, companies are using AI in recruitment and other HR functions including pay and promotion, technologies including video-analysis, robot interviews and conversation analysis. They found that there is a lack of specific regulation to prevent discrimination from AI systems, and noted that the intrusive nature of biometric technologies such as facial recognition may be particularly difficult (and even impossible) to justify in 'more mundane commercial contexts'[197] as compared, for example, to law enforcement contexts where personal safety may be positively impacted by the deployment of the technology.

8.94 Each of these factors warrants further careful consideration. We recommend the commissioning of further, private-sector focused work to achieve this.

197 Allen QC, R. and Masters, D. (2021). *Technology Managing People – the legal implications.* TUC. Available at: https://www.tuc.org.uk/sites/default/files/Technology_Managing_People_2021_Report_AW_0.pdf

Annex 1: Legal provisions

This Annex contains extracts from the materials that currently provide law and regulation relating to biometric data relevant to the UK, and are referred to in the body of the Review.

Data Protection Act 2018

Section 3 – Terms relating to the processing of personal data

[...]

(2) "Personal data" means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

(4) "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as—

(a) collection, recording, organisation, structuring or storage,
(b) adaptation or alteration,
(c) retrieval, consultation or use,
(d) disclosure by transmission, dissemination or otherwise making available,
(e) alignment or combination, or
(f) restriction, erasure or destruction,

(subject to subsection (14)(c) and sections 5(7), 29(2) and 82(3), which make provision about references to processing in the different Parts of this Act).

Section 10 – Special categories of personal data and criminal convictions etc data

(1) Subsections (2) and (3) make provision about the processing of personal data described in Article 9(1) of the UK GDPR (prohibition on processing of special categories of personal data) in reliance on an exception in one of the following points of Article 9(2)—

(a) point (b) (employment, social security and social protection);
(b) point (g) (substantial public interest);
(c) point (h) (health and social care);
(d) point (i) (public health);
(e) point (j) (archiving, research and statistics).

(2) The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the UK GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

(3) The processing meets the requirement in point (g) of Article 9(2) of the UK GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

(4) Subsection (5) makes provision about the processing of personal data relating to criminal convictions and offences or related security measures that is not carried out under the control of official authority.

(5) The processing meets the requirement in Article 10 of the UK GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.

(6) The Secretary of State may by regulations—

(a) amend Schedule 1—

(i) by adding or varying conditions or safeguards, and
(ii) by omitting conditions or safeguards added by regulations under this section, and

(b) consequentially amend this section.

(7) Regulations under this section are subject to the affirmative resolution procedure.

Section 30 – Meaning of "competent authority"

(1) In this Part, "competent authority" means—

(a) a person specified or described in Schedule 7, and
(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

(2) But an intelligence service is not a competent authority within the meaning of this Part.

[...]

(7) In this section—

"intelligence service" means—

(a) the Security Service;
(b) the Secret Intelligence Service;
(c) the Government Communications Headquarters;

Section 31 – "The law enforcement purposes"

For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

Section 35 – The first data protection principle

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

(2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or
(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

(3) In addition, where the processing for any of the law enforcement purposes is sensitive processing, the processing is permitted only in the two cases set out in subsections (4) and (5).

(4) The first case is where—

(a) the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and
(b) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

(5) The second case is where—

(a) the processing is strictly necessary for the law enforcement purpose,
(b) the processing meets at least one of the conditions in Schedule 8, and
(c) at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

[...]

(8) In this section, "sensitive processing" means—

[...]

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

Section 36 – The second data protection principle

(1) The second data protection principle is that—

(a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that—

(a) the controller is authorised by law to process the data for the other purpose, and
(b) the processing is necessary and proportionate to that other purpose.

(4) Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

Section 37 – The third data protection principle

The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Section 38 – The fourth data protection principle

(1) The fourth data protection principle is that—

(a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and
(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(2) In processing personal data for any of the law enforcement purposes, personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments.

(3) In processing personal data for any of the law enforcement purposes, a clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as—

(a) persons suspected of having committed or being about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) persons who are or may be victims of a criminal offence;
(d) witnesses or other persons with information about offences.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose—

(a) the quality of personal data must be verified before it is transmitted or made available,
(b) in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included, and
(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Section 39 – The fifth data protection principle

(1) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Section 40 – The sixth data protection principle

The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Section 82 – Processing to which this Part applies

[...]

(2) In this Part, "intelligence service" means—

(a) the Security Service;
(b) the Secret Intelligence Service;
(c) the Government Communications Headquarters.

Section 86 – The first data protection principle

[...]

(2) The processing of personal data is lawful only if and to the extent that—

[...]

(b) in the case of sensitive processing, at least one of the conditions in Schedule 10 is also met.

[...]

(7) In this section, "sensitive processing" means—

(c) the processing of biometric data for the purpose of uniquely identifying an individual;

Section 87 – The second data protection principle

(1) The second data protection principle is that—

(a) the purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and
(b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

(2) Paragraph (b) of the second data protection principle is subject to subsections (3) and (4).

(3) Personal data collected by a controller for one purpose may be processed for any other purpose of the controller that collected the data or any purpose of another controller provided that—

(a) the controller is authorised by law to process the data for that purpose, and
(b) the processing is necessary and proportionate to that other purpose.

(4) Processing of personal data is to be regarded as compatible with the purpose for which it is collected if the processing—

(a) consists of—

(i) processing for archiving purposes in the public interest,
(ii) processing for the purposes of scientific or historical research, or
(iii) processing for statistical purposes, and

(b) is subject to appropriate safeguards for the rights and freedoms of the data subject.

Section 88 – The third data protection principle

The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Section 89 – The fourth data protection principle

The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

Section 90 – The fifth data protection principle

The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

Section 91 – The sixth data protection principle

(1) The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.

(2) The risks referred to in subsection (1) include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

Section 205 – General interpretation

(1) In this Act—

> "biometric data" means 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 data;

Schedule 7: Competent authorities

Paragraph 1

> Any United Kingdom government department other than a non-ministerial government department.

[...]

Paragraph 5

The chief constable of a police force maintained under section 2 of the Police Act 1996.

Paragraph 6

The Commissioner of Police of the Metropolis.

Paragraph 7

The Commissioner of Police for the City of London.

[...]

Paragraph 10

The chief constable of the British Transport Police.

Paragraph 11

The chief constable of the Civil Nuclear Constabulary.

Paragraph 12

The chief constable of the Ministry of Defence Police.

Paragraph 13

The Provost Marshal of the Royal Navy Police.

Paragraph 14

The Provost Marshal of the Royal Military Police.

Paragraph 15

The Provost Marshal of the Royal Air Force Police.

Paragraph 16

The chief officer of—

(a) a body of constables appointed under provision incorporating section 79 of the Harbours, Docks, and Piers Clauses Act 1847;
(b) a body of constables appointed under an order made under section 14 of the Harbours Act 1964;
(c) the body of constables appointed under section 154 of the Port of London Act 1968.

Paragraph 17

A body established in accordance with a collaboration agreement under section 22A of the Police Act 1996.

Paragraph 18

The Director General of the Independent Office for Police Conduct.

[...]

Paragraph 21

The Commissioners for Her Majesty's Revenue and Customs.

Paragraph 24

The Director General of the National Crime Agency.

Paragraph 25

The Director of the Serious Fraud Office.

Paragraph 26

The Director of Border Revenue.

Paragraph 27

The Financial Conduct Authority.

Paragraph 28

The Health and Safety Executive.

Paragraph 29

The Competition and Markets Authority.

Paragraph 30

The Gas and Electricity Markets Authority.

Paragraph 31

The Food Standards Agency.

[...]

Paragraph 33

Her Majesty's Land Registry.

Paragraph 34

The Criminal Cases Review Commission.

[...]

Paragraph 36

A provider of probation services (other than the Secretary of State), acting in pursuance of arrangements made under section 3(2) of the Offender Management Act 2007.

Paragraph 37

The Youth Justice Board for England and Wales.

Paragraph 38

The Parole Board for England and Wales.

[...]

Paragraph 43

A person who has entered into a contract for the running of, or part of—

(a) a prison or young offender institution under section 84 of the Criminal Justice Act 1991, or
(b) a secure training centre under section 7 of the Criminal Justice and Public Order Act 1994.

Paragraph 44

A person who has entered into a contract with the Secretary of State—

(a) under section 80 of the Criminal Justice Act 1991 for the purposes of prisoner escort arrangements, or
(b) under paragraph 1 of Schedule 1 to the Criminal Justice and Public Order Act 1994 for the purposes of escort arrangements.

Paragraph 45

A person who is, under or by virtue of any enactment, responsible for securing the electronic monitoring of an individual.

Paragraph 46

A youth offending team established under section 39 of the Crime and Disorder Act 1998.

Paragraph 47

The Director of Public Prosecutions.

[...]

Paragraph 52

The Information Commissioner.

[...]

Paragraph 55

The Crown agent.

Paragraph 56

A court or tribunal.

Schedule 8 – Conditions for sensitive processing under Part 3

Paragraph 1

This condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and
(b) is necessary for reasons of substantial public interest.

Paragraph 2

This condition is met if the processing is necessary for the administration of justice.

Paragraph 3

This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

Paragraph 4

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or
(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or
(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and
(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,
(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and
(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Paragraph 5

This condition is met if the processing relates to personal data which is manifestly made public by the data subject.

Paragraph 6

This condition is met if the processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Paragraph 7

This condition is met if the processing is necessary when a court or other judicial authority is acting in its judicial capacity.

Paragraph 8

(1) This condition is met if the processing—

(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and
(b) consists of—

(i) the disclosure of personal data by a competent authority as a member of an anti-fraud organisation,
(ii) the disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation, or
(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

Paragraph 9

This condition is met if the processing is necessary—

(a) for archiving purposes in the public interest,
(b) for scientific or historical research purposes, or
(c) for statistical purposes.

Schedule 9 – Conditions for processing under Part 4

Paragraph 1

The data subject has given consent to the processing.

Paragraph 2

The processing is necessary—

(a) for the performance of a contract to which the data subject is a party, or
(b) in order to take steps at the request of the data subject prior to entering into a contract.

Paragraph 3

The processing is necessary for compliance with a legal obligation to which the controller is subject, other than an obligation imposed by contract.

Paragraph 4

The processing is necessary in order to protect the vital interests of the data subject or of another individual.

Paragraph 5

The processing is necessary—

(a) for the administration of justice,
(b) for the exercise of any functions of either House of Parliament,
(c) for the exercise of any functions conferred on a person by an enactment or rule of law,
(d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(e) for the exercise of any other functions of a public nature exercised in the public interest by a person.

Paragraph 6

(1) The processing is necessary for the purposes of legitimate interests pursued by—

(a) the controller, or
(b) the third party or parties to whom the data is disclosed.

(2) Sub-paragraph (1) does not apply where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

(3) In this paragraph, "third party", in relation to personal data, means a person other than the data subject, the controller or a processor or other person authorised to process personal data for the controller or processor.

Schedule 10 – Conditions for sensitive processing under Part 4

Paragraph 1

The data subject has given consent to the processing.

Paragraph 2

The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by an enactment or rule of law on the controller in connection with employment.

Paragraph 3

The processing is necessary—

(a) in order to protect the vital interests of the data subject or of another person, in a case where—

(i) consent cannot be given by or on behalf of the data subject, or
(ii) the controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Paragraph 4

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or
(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or
(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and
(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and
(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

Paragraph 5

The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Paragraph 6

The processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Paragraph 7

The processing is necessary—

(a) for the administration of justice,
(b) for the exercise of any functions of either House of Parliament,
(c) for the exercise of any functions conferred on any person by an enactment or rule of law, or
(d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Paragraph 8

(1) The processing is necessary for medical purposes and is undertaken by—

(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph, "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

Paragraph 9

(1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) In this paragraph, "sensitive personal data" means personal data the processing of which constitutes sensitive processing (see section 86(7)).

UK General Data Protection Regulation ('GDPR')

Article 4 – Definitions

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

[...]

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;[...]

Article 5 – Principles relating to processing of personal data

(1) Personal data shall be:

[...]

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); [...]

Article 9 – Processing of special categories of personal data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(2) Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to

the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under domestic law or rules established by national competent bodies.

(3A) In paragraph 3, 'national competent bodies' means competent bodies of the United Kingdom or a part of the United Kingdom.

[...]

(5) In the 2018 Act-

(a) section 10 makes provision about when the requirement in paragraph 2(b), (g), (h), (i) or (j) of this Article for authorisation by, or a basis in, domestic law is met;
(b) section 11(1) makes provision about when the processing of personal data is carried out in circumstances described in paragraph 3 of this Article.

Human Rights Act 1998

Section 1 – The Convention Rights

(1) In this Act "the Convention rights" means the rights and fundamental freedoms set out in—

(a) Articles 2 to 12 and 14 of the Convention,
(b) Articles 1 to 3 of the First Protocol, and
(c) Article 1 of the Thirteenth Protocol, as read with Articles 16 to 18 of the Convention.

(2) Those Articles are to have effect for the purposes of this Act subject to any designated derogation or reservation (as to which see sections 14 and 15).

(3) The Articles are set out in Schedule 1.

Section 6 – Acts of public authorities

(1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right.

(2) Subsection (1) does not apply to an act if—

(a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or
(b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions.

(3) In this section "public authority" includes—

(a) a court or tribunal, and
(b) any person certain of whose functions are functions of a public nature, [...]

Schedule 1, Article 8 – Right to respect for private and family life

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Police and Criminal Evidence Act 1984

Section 61 — Finger-printing

(1) Except as provided by this section no person's fingerprints may be taken without the appropriate consent.

(2) Consent to the taking of a person's fingerprints must be in writing if it is given at a time when he is at a police station.

(3) The fingerprints of a person detained at a police station may be taken without the appropriate consent if—

> (a) he is detained in consequence of his arrest for a recordable offence; and
> (b) he has not had his fingerprints taken in the course of the investigation of the offence by the police.

(3A) Where a person mentioned in paragraph (a) of subsection (3) or (4) has already had his fingerprints taken in the course of the investigation of the offence by the police, that fact shall be disregarded for the purposes of that subsection if–

> (a) the fingerprints taken on the previous occasion do not constitute a complete set of his fingerprints; or
> (b) some or all of the fingerprints taken on the previous occasion are not of sufficient quality to allow satisfactory analysis, comparison or matching (whether in the case in question or generally).

(4) The fingerprints of a person detained at a police station may be taken without the appropriate consent if—

(a) he has been charged with a recordable offence or informed that he will be reported for such an offence; and
(b) he has not had his fingerprints taken in the course of the investigation of the offence by the police.

(4A) The fingerprints of a person who has answered to bail at a court or police station may be taken without the appropriate consent at the court or station if–

(a) the court, or
(b) an officer of at least the rank of inspector,
authorises them to be taken.

(4B) A court or officer may only give an authorisation under subsection (4A) if–

(a) the person who has answered to bail has answered to it for a person whose fingerprints were taken on a previous occasion and there are reasonable grounds for believing that he is not the same person; or
(b) the person who has answered to bail claims to be a different person from a person whose fingerprints were taken on a previous occasion.

(5) An officer may give an authorisation under subsection (4A) above orally or in writing but, if he gives it orally, he shall confirm it in writing as soon as is practicable.

(5A) The fingerprints of a person may be taken without the appropriate consent if (before or after the coming into force of this subsection) he has been arrested for a recordable offence and released and—

(a) he has not had his fingerprints taken in the course of the investigation of the offence by the police; or
(b) he has had his fingerprints taken in the course of that investigation but

(i) subsection (3A)(a) or (b) above applies, or

(ii) subsection (5C) below applies.

(5B) The fingerprints of a person not detained at a police station may be taken without the appropriate consent if (before or after the coming into force of this subsection) he has been charged with a recordable offence or informed that he will be reported for such an offence and—

(a) he has not had his fingerprints taken in the course of the investigation of the offence by the police; or
(b) he has had his fingerprints taken in the course of that investigation but

(i) subsection (3A)(a) or (b) above applies, or
(ii) subsection (5C) below applies.

(5C) This subsection applies where—

(a) the investigation was discontinued but subsequently resumed, and
(b) before the resumption of the investigation the fingerprints were destroyed pursuant to section 63D(3) below.

(6) Subject to this section, the fingerprints of a person may be taken without the appropriate consent if (before or after the coming into force of this subsection)—

(a) he has been convicted of a recordable offence, or
(b) he has been given a caution in respect of a recordable offence which, at the time of the caution, he has admitted, and either of the conditions mentioned in subsection (6ZA) below is met.

(6ZA) The conditions referred to in subsection (6) above are—

(a) the person has not had his fingerprints taken since he was convicted or cautioned;
(b) he has had his fingerprints taken since then but subsection (3A)(a) or (b) above applies.

(6ZB) Fingerprints may only be taken as specified in subsection (6) above with the authorisation of an officer of at least the rank of inspector.

(6ZC) An officer may only give an authorisation under subsection (6ZB) above if the officer is satisfied that taking the fingerprints is necessary to assist in the prevention or detection of crime.

(6A) A constable may take a person's fingerprints without the appropriate consent if—

(a) the constable reasonably suspects that the person is committing or attempting to commit an offence, or has committed or attempted to commit an offence; and
(b) either of the two conditions mentioned in subsection (6B) is met.

(6B) The conditions are that—

(a) the name of the person is unknown to, and cannot be readily ascertained by, the constable;
(b) the constable has reasonable grounds for doubting whether a name furnished by the person as his name is his real name.

(6C) The taking of fingerprints by virtue of subsection (6A) does not count for any of the purposes of this Act as taking them in the course of the investigation of an offence by the police.

(6D) Subject to this section, the fingerprints of a person may be taken without the appropriate consent if—

(a) under the law in force in a country or territory outside England and Wales the person has been convicted of an offence under that law (whether before or after the coming into force of this subsection and whether or not he has been punished for it);
(b) the act constituting the offence would constitute a qualifying offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted); and
(c) either of the conditions mentioned in subsection (6E) below is met.

(6E) The conditions referred to in subsection (6D)(c) above are—

(a) the person has not had his fingerprints taken on a previous occasion under subsection (6D) above;

(b) he has had his fingerprints taken on a previous occasion under that subsection but subsection (3A)(a) or (b) above applies.

(6F) Fingerprints may only be taken as specified in subsection (6D) above with the authorisation of an officer of at least the rank of inspector.

(6G) An officer may only give an authorisation under subsection (6F) above if the officer is satisfied that taking the fingerprints is necessary to assist in the prevention or detection of crime.

(7) Where a person's fingerprints are taken without the appropriate consent by virtue of any power conferred by this section—

(a) before the fingerprints are taken, the person shall be informed of—

(i) the reason for taking the fingerprints;
(ii) the power by virtue of which they are taken; and
(iii) in a case where the authorisation of the court or an officer is required for the exercise of the power, the fact that the authorisation has been given; and

(b) those matters shall be recorded as soon as practicable after the fingerprints are taken.

(7A) If a person's fingerprints are taken at a police station, or by virtue of subsection (4A), (6A) at a place other than a police station, whether with or without the appropriate consent—

(a) before the fingerprints are taken, an officer shall inform him that they may be the subject of a speculative search; and
(b) the fact that the person has been informed of this possibility shall be recorded as soon as is practicable after the fingerprints have been taken.

(8) If he is detained at a police station when the fingerprints are taken, the matters referred to in subsection (7)(a)(i) to (iii) above and, in the case falling within subsection (7A) above, the fact referred to in paragraph (b) of that subsection shall be recorded on his custody record.

(8B) Any power under this section to take the fingerprints of a person without the appropriate consent, if not otherwise specified to be exercisable by a constable, shall be exercisable by a constable.

(9) Nothing in this section—

(a) affects any power conferred by paragraph 18(2) of Schedule 2 to the Immigration Act 1971; or
(b) applies to a person arrested or detained under the terrorism provisions or detained under Part 1 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019.

(10) Nothing in this section applies to a person arrested under an extradition arrest power.

Section 62 – Intimate samples

(1) Subject to section 63B below an intimate sample may be taken from a person in police detention only—

(a) if a police officer of at least the rank of inspector authorises it to be taken; and
(b) if the appropriate consent is given.

(1A) An intimate sample may be taken from a person who is not in police detention but from whom, in the course of the investigation of an offence, two or more non-intimate samples suitable for the same means of analysis have been taken which have proved insufficient—

(a) if a police officer of at least the rank of inspector authorises it to be taken; and
(b) if the appropriate consent is given.

(2) An officer may only give an authorisation under subsection (1) or (1A) above if he has reasonable grounds—

(a) for suspecting the involvement of the person from whom the sample is to be taken in a recordable offence; and
(b) for believing that the sample will tend to confirm or disprove his involvement.

(2A) An intimate sample may be taken from a person where—

(a) two or more non-intimate samples suitable for the same means of analysis have been taken from the person under section 63(3E) below (persons convicted of offences outside England and Wales etc) but have proved insufficient;
(b) a police officer of at least the rank of inspector authorises it to be taken; and
(c) the appropriate consent is given.

(2B) An officer may only give an authorisation under subsection (2A) above if the officer is satisfied that taking the sample is necessary to assist in the prevention or detection of crime.

(3) An officer may give an authorisation under subsection (1) or (1A) or (2A) above orally or in writing but, if he gives it orally, he shall confirm it in writing as soon as is practicable.

(4) The appropriate consent must be given in writing.

(5) Before an intimate sample is taken from a person, an officer shall inform him of the following—

(a) the reason for taking the sample;
(b) the fact that authorisation has been given and the provision of this section under which it has been given; and
(c) if the sample was taken at a police station, the fact that the sample may be the subject of a speculative search.

(6) The reason referred to in subsection (5)(a) above must include, except in a case where the sample is taken under subsection (2A) above, a statement of the nature of the offence in which it is suspected that the person has been involved.

(7) After an intimate sample has been taken from a person, the following shall be recorded as soon as practicable—

(a) the matters referred to in subsection (5)(a) and (b) above;
(b) if the sample was taken at a police station, the fact that the person has been informed as specified in subsection (5)(c) above; and
(c) the fact that the appropriate consent was given.

(8) If an intimate sample is taken from a person detained at a police station, the matters required to be recorded by subsection (7) above shall be recorded in his custody record.

(9) In the case of an intimate sample which is a dental impression, the sample may be taken from a person only by a registered dentist.

(9A) In the case of any other form of intimate sample, except in the case of a sample of urine, the sample may be taken from a person only by—

(a) a registered medical practitioner; or
(b) a registered health care professional.

(10) Where the appropriate consent to the taking of an intimate sample from a person was refused without good cause, in any proceedings against that person for an offence—

(a) the court, in determining–

(ii) whether there is a case to answer; and

(aa) a judge, in deciding whether to grant an application made by the accused under paragraph 2 of Schedule 3 to the Crime and Disorder Act 1998 (applications for dismissal); and
(b) the court or jury, in determining whether that person is guilty of the offence charged,
may draw such inferences from the refusal as appear proper.

(11) Nothing in this section applies to the taking of a specimen for the purposes of any of the provisions of sections 4 to 11 of the Road Traffic Act 1988 or of sections 26 to 38 of the Transport and Works Act 1992.

(12) Nothing in this section applies to a person arrested or detained under the terrorism provisions; and subsection (1A) shall not apply where the non-intimate samples mentioned in that subsection were taken under paragraph 10 of Schedule 8 to the Terrorism Act 2000.

(13) Nothing in this section applies to a person detained under Part 1 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019; and subsection (1A) does not apply where the non-intimate

samples mentioned in that subsection were taken under Part 2 of that Schedule.

Section 63 – Other samples

(1) Except as provided by this section, a non-intimate sample may not be taken from a person without the appropriate consent.

(2) Consent to the taking of a non-intimate sample must be given in writing.

(2A) A non-intimate sample may be taken from a person without the appropriate consent if two conditions are satisfied.

(2B) The first is that the person is in police detention in consequence of his arrest for a recordable offence.

(2C) The second is that—

> (a) he has not had a non-intimate sample of the same type and from the same part of the body taken in the course of the investigation of the offence by the police, or
> (b) he has had such a sample taken but it proved insufficient.

(3) A non-intimate sample may be taken from a person without the appropriate consent if—

> (a) he is being held in custody by the police on the authority of a court; and
> (b) an officer of at least the rank of inspector authorises it to be taken without the appropriate consent.

(3ZA) A non-intimate sample may be taken from a person without the appropriate consent if (before or after the coming into force of this subsection) he has been arrested for a recordable offence and released and—

> (a) he has not had a nonintimate sample of the same type and from the same part of the body taken from him in the course of the investigation of the offence by the police; or
> (b) he has had a non-intimate sample taken from him in the

course of that investigation but—

(i) it was not suitable for the same means of analysis, or
(ii) it proved insufficient, or
(iii) subsection (3AA) below applies.

(3A) A non-intimate sample may be taken from a person (whether or not he is in police detention or held in custody by the police on the authority of a court) without the appropriate consent if he has been charged with a recordable offence or informed that he will be reported for such an offence and—

(a) he has not had a non-intimate sample taken from him in the course of the investigation of the offence by the police; or
(b) he has had a non-intimate sample taken from him in the course of that investigation but—

(i) it was not suitable for the same means of analysis, or
(ii) it proved insufficient, or
(iii) subsection (3AA) below applies; or

(c) he has had a non-intimate sample taken from him in the course of that investigation and—

(i) the sample has been destroyed pursuant to section 63R below or any other enactment, and
(ii) it is disputed, in relation to any proceedings relating to the offence, whether a DNA profile relevant to the proceedings is derived from the sample.

(3AA) This subsection applies where the investigation was discontinued but subsequently resumed, and before the resumption of the investigation—

(a) any DNA profile derived from the sample was destroyed pursuant to section 63D(3) below, and
(b) the sample itself was destroyed pursuant to section 63R(4), (5) or (12) below.

(3B) Subject to this section, a non-intimate sample may be taken from a person without the appropriate consent if (before or after the coming into force of this subsection)—

(a) he has been convicted of a recordable offence, or
(b) he has been given a caution in respect of a recordable offence which, at the time of the caution, he has admitted, and either of the conditions mentioned in subsection (3BA) below is met.

(3BA) The conditions referred to in subsection (3B) above are—

(a) a non-intimate sample has not been taken from the person since he was convicted or cautioned;
(b) such a sample has been taken from him since then but—

(i) it was not suitable for the same means of analysis, or
(ii) it proved insufficient.

(3BB) A non-intimate sample may only be taken as specified in subsection (3B) above with the authorisation of an officer of at least the rank of inspector.

(3BC) An officer may only give an authorisation under subsection (3BB) above if the officer is satisfied that taking the sample is necessary to assist in the prevention or detection of crime.

(3C) A non-intimate sample may also be taken from a person without the appropriate consent if he is a person to whom section 2 of the Criminal Evidence (Amendment) Act 1997 applies (persons detained following acquittal on grounds of insanity or finding of unfitness to plead).

(3E) Subject to this section, a non-intimate sample may be taken without the appropriate consent from a person if—

(a) under the law in force in a country or territory outside England and Wales the person has been convicted of an offence under that law (whether before or after the coming into force of this subsection and whether or not he has been punished for it);
(b) the act constituting the offence would constitute a qualifying offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted); and
(c) either of the conditions mentioned in subsection (3F) below is met.

(3F) The conditions referred to in subsection (3E)(c) above are—

(a) the person has not had a non-intimate sample taken from him on a previous occasion under subsection (3E) above;
(b) he has had such a sample taken from him on a previous occasion under that subsection but—

(i) the sample was not suitable for the same means of analysis, or
(ii) it proved insufficient.

(3G) A non-intimate sample may only be taken as specified in subsection (3E) above with the authorisation of an officer of at least the rank of inspector.

(3H) An officer may only give an authorisation under subsection (3G) above if the officer is satisfied that taking the sample is necessary to assist in the prevention or detection of crime.

(4) An officer may only give an authorisation under subsection (3) above if he has reasonable grounds—

(a) for suspecting the involvement of the person from whom the sample is to be taken in a recordable offence; and
(b) for believing that the sample will tend to confirm or disprove his involvement.

(5) An officer may give an authorisation under subsection (3) above orally or in writing but, if he gives it orally, he shall confirm it in writing as soon as is practicable.

(5A) An officer shall not give an authorisation under subsection (3) above for the taking from any person of a non-intimate sample consisting of a skin impression if–

(a) a skin impression of the same part of the body has already been taken from that person in the course of the investigation of the offence; and
(b) the impression previously taken is not one that has proved insufficient.

(6) Where a non-intimate sample is taken from a person without the appropriate consent by virtue of any power conferred by this section—

(a) before the sample is taken, an officer shall inform him of—

(i) the reason for taking the sample;
(ii) the power by virtue of which it is taken; and
(iii) in a case where the authorisation of an officer is required for the exercise of the power, the fact that the authorisation has been given; and

(b) those matters shall be recorded as soon as practicable after the sample is taken.

(7) The reason referred to in subsection (6)(a)(i) above must include, except in a case where the non-intimate sample is taken under subsection (3B) or (3E) above, a statement of the nature of the offence in which it is suspected that the person has been involved.

(8B) If a non-intimate sample is taken from a person at a police station, whether with or without the appropriate consent—

(a) before the sample is taken, an officer shall inform him that it may be the subject of a speculative search; and
(b) the fact that the person has been informed of this possibility shall be recorded as soon as practicable after the sample has been taken.

(9) If a non-intimate sample is taken from a person detained at a police station, the matters required to be recorded by subsection (6) or (8B) above shall be recorded in his custody record.

(9ZA) The power to take a non-intimate sample from a person without the appropriate consent shall be exercisable by any constable.

(9A) Subsection (3B) above shall not apply to –

(a) any person convicted before 10th April 1995 unless he is a person to whom section 1 of the Criminal Evidence (Amendment) Act 1997 applies (persons imprisoned or detained

by virtue of pre-existing conviction for sexual offence etc.); or
(b) a person given a caution before 10th April 1995.

(10) Nothing in this section applies to a person arrested or detained under the terrorism provisions or detained under Part 1 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019.

(11) Nothing in this section applies to a person arrested under an extradition arrest power.

Section 63D – Destruction of fingerprints and DNA profiles

(1) This section applies to—

(a) fingerprints—

(i) taken from a person under any power conferred by this Part of this Act, or
(ii) taken by the police, with the consent of the person from whom they were taken, in connection with the investigation of an offence by the police, and

(b) a DNA profile derived from a DNA sample taken as mentioned in paragraph (a)(i) or (ii).

(2) Fingerprints and DNA profiles to which this section applies ("section 63D material") must be destroyed if it appears to the responsible chief officer of police that—

(a) the taking of the fingerprint or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful, or
(b) the fingerprint was taken, or, in the case of a DNA profile, was derived from a sample taken, from a person in connection with that person's arrest and the arrest was unlawful or based on mistaken identity.

(3) In any other case, section 63D material must be destroyed unless it is retained under any power conferred by sections 63E to 63O (including those sections as applied by section 63P).

(4) Section 63D material which ceases to be retained under a power mentioned in subsection (3) may continue to be retained under any other such power which applies to it.

(5) Nothing in this section prevents a speculative search, in relation to section 63D material, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

Section 63E – Retention of section 63D material pending investigation or proceedings

(1) This section applies to section 63D material taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of an offence in which it is suspected that the person to whom the material relates has been involved.

(2) The material may be retained until the conclusion of the investigation of the offence or, where the investigation gives rise to proceedings against the person for the offence, until the conclusion of those proceedings.

Section 63F – Retention of section 63D material: persons arrested for or charged with a qualifying offence

(1) This section applies to section 63D material which—

(a) relates to a person who is arrested for, or charged with, a qualifying offence but is not convicted of that offence, and
(b) was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence.

(2) If the person has previously been convicted of a recordable offence which is not an excluded offence, or is so convicted before the material is required to be destroyed by virtue of this section, the material may be retained indefinitely.

(2A) In subsection (2), references to a recordable offence include an offence under the law of a country or territory outside England

and Wales where the act constituting the offence would constitute a recordable offence if done in England and Wales (and, in the application of subsection (2) where a person has previously been convicted, this applies whether or not the act constituted such an offence when the person was convicted).

(3) Otherwise, material falling within subsection (4), (5) or (5A) may be retained until the end of the retention period specified in subsection (6).

(4) Material falls within this subsection if it—

(a) relates to a person who is charged with a qualifying offence but is not convicted of that offence, and
(b) was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence.

(5) Material falls within this subsection if—

(a) it relates to a person who is arrested for a qualifying offence, other than a terrorism-related qualifying offence, but is not charged with that offence,
(b) it was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence, and

(c) the Commissioner for the Retention and Use of Biometric Material has consented under section 63G to the retention of the material.

(5A) Material falls within this subsection if—

(a) it relates to a person who is arrested for a terrorism-related qualifying offence but is not charged with that offence, and
(b) it was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence.

(6) The retention period is—

(a) in the case of fingerprints, the period of 3 years beginning

with the date on which the fingerprints were taken, and
(b) in the case of a DNA profile, the period of 3 years beginning with the date on which the DNA sample from which the profile was derived was taken (or, if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken).

(7) The responsible chief officer of police or a specified chief officer of police may apply to a District Judge (Magistrates' Courts) for an order extending the retention period.

(8) An application for an order under subsection (7) must be made within the period of 3 months ending on the last day of the retention period.

(9) An order under subsection (7) may extend the retention period by a period which—

(a) begins with the end of the retention period, and
(b) ends with the end of the period of 2 years beginning with the end of the retention period.

(10) The following persons may appeal to the Crown Court against an order under subsection (7), or a refusal to make such an order—

(a) the responsible chief officer of police;
(b) a specified chief officer of police;
(c) the person from whom the material was taken.

(11) In this section—

"excluded offence", in relation to a person, means a recordable offence—

(a) which—

(i) is not a qualifying offence,
(ii) is the only recordable offence of which the person has been convicted, and
(iii) was committed when the person was aged under 18, and

(b) for which the person was not given a relevant custodial sentence of 5 years or more,

"relevant custodial sentence" has the meaning given by section 63K(6),

"a specified chief officer of police" means—

(a) the chief officer of the police force of the area in which the person from whom the material was taken resides, or
(b) a chief officer of police who believes that the person is in, or is intending to come to, the chief officer's police area.

"terrorism-related qualifying offence" means—

(a) an offence for the time being listed in section 41(1) of the Counter-Terrorism Act 2008 (see section 65A(2)(r) below), or
(b) an ancillary offence, as defined by section 65A(5) below, relating to an offence for the time being listed in section 41(1) of that Act.

(12) For the purposes of the definition of "excluded offence" in subsection (11)—

(a) references to a recordable offence or a qualifying offence include an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence or (as the case may be) a qualifying offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted), and

(b) in the application of paragraph (b) of that definition in relation to an offence under the law of a country or territory outside England and Wales, the reference to a relevant custodial sentence of 5 years or more is to be read as a reference to a sentence of imprisonment or other form of detention of 5 years or more.

Section 63G – Retention of section 63D material by virtue of section 63F(5): consent of Commissioner

(1) The responsible chief officer of police may apply under subsection (2) or (3) to the Commissioner for the Retention and Use of Biometric Material for consent to the retention of section 63D material which falls within section 63F(5)(a) and (b).

(2) The responsible chief officer of police may make an application under this subsection if the responsible chief officer of police considers that the material was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of an offence where any alleged victim of the offence was, at the time of the offence—

(a) under the age of 18,
(b) a vulnerable adult, or
(c) associated with the person to whom the material relates.

(3) The responsible chief officer of police may make an application under this subsection if the responsible chief officer of police considers that—

(a) the material is not material to which subsection (2) relates, but
(b) the retention of the material is necessary to assist in the prevention or detection of crime.

(4) The Commissioner may, on an application under this section, consent to the retention of material to which the application relates if the Commissioner considers that it is appropriate to retain the material.

(5) But where notice is given under subsection (6) in relation to the application, the Commissioner must, before deciding whether or not to give consent, consider any representations by the person to whom the material relates which are made within the period of 28 days beginning with the day on which the notice is given.

(6) The responsible chief officer of police must give to the person to whom the material relates notice of—

(a) an application under this section, and
(b) the right to make representations.

(7) A notice under subsection (6) may, in particular, be given to a person by—

(a) leaving it at the person's usual or last known address (whether residential or otherwise),
(b) sending it to the person by post at that address, or
(c) sending it to the person by email or other electronic means.

(8) The requirement in subsection (6) does not apply if the whereabouts of the person to whom the material relates is not known and cannot, after reasonable inquiry, be ascertained by the responsible chief officer of police.

(9) An application or notice under this section must be in writing.

(10) In this section—

"victim" includes intended victim,

"vulnerable adult" means a person aged 18 or over whose ability to protect himself or herself from violence, abuse or neglect is significantly impaired through physical or mental disability or illness, through old age or otherwise,

and the reference in subsection (2)(c) to a person being associated with another person is to be read in accordance with section 62(3) to (7) of the Family Law Act 1996.

Section 63H – Retention of section 63D material: persons arrested for or charged with a minor offence

(1) This section applies to section 63D material which—

(a) relates to a person who—

(i) is arrested for or charged with a recordable offence other than a qualifying offence,
(ii) if arrested for or charged with more than one offence

arising out of a single course of action, is not also arrested for or charged with a qualifying offence, and
(iii) is not convicted of the offence or offences in respect of which the person is arrested or charged, and

(b) was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence or offences in respect of which the person is arrested or charged.

(2) If the person has previously been convicted of a recordable offence which is not an excluded offence, the material may be retained indefinitely.

(2A) In subsection (2), the reference to a recordable offence includes an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted).

(3) In this section "excluded offence" has the meaning given by section 63F (11) (read with section 63F(12)).

Section 63I – Retention of material: persons convicted of a recordable offence

(1) This section applies, subject to subsection (3), to—

(a) section 63D material which—

(i) relates to a person who is convicted of a recordable offence, and
(ii) was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence, or

(b) material taken under section 61(6) or 63(3B) which relates to a person who is convicted of a recordable offence.

(2) The material may be retained indefinitely.

(3) This section does not apply to section 63D material to which section 63K applies.

Section 63J – Retention of material: persons convicted of an offence outside England and Wales: other cases

(1) This section applies to material falling within subsection (2) relating to a person who is convicted of an offence under the law of any country or territory outside England and Wales.

(2) Material falls within this subsection if it is—

(a) fingerprints taken from the person under section 61(6D) (power to take fingerprints without consent in relation to offences outside England and Wales), or
(b) a DNA profile derived from a DNA sample taken from the person under section 62(2A) or 63(3E) (powers to take intimate and non-intimate samples in relation to offences outside England and Wales).

(3) The material may be retained indefinitely.

Section 63K – Retention of section 63D material: exception for persons under 18 convicted of first minor offence

(1) This section applies to section 63D material which—

(a) relates to a person who—

(i) is convicted of a recordable offence other than a qualifying offence,
(ii) has not previously been convicted of a recordable offence, and
(iii) is aged under 18 at the time of the offence, and

(b) was taken (or, in the case of a DNA profile, derived from a sample taken) in connection with the investigation of the offence.

(1A) In subsection (1)(a)(ii), the reference to a recordable offence includes an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted).

(2) Where the person is given a relevant custodial sentence of less than 5 years in respect of the offence, the material may be retained until the end of the period consisting of the term of the sentence plus 5 years.

(3) Where the person is given a relevant custodial sentence of 5 years or more in respect of the offence, the material may be retained indefinitely.

(4) Where the person is given a sentence other than a relevant custodial sentence in respect of the offence, the material may be retained until—

(a) in the case of fingerprints, the end of the period of 5 years beginning with the date on which the fingerprints were taken, and
(b) in the case of a DNA profile, the end of the period of 5 years beginning with—

(i) the date on which the DNA sample from which the profile was derived was taken, or
(ii) if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken.

(5) But if, before the end of the period within which material may be retained by virtue of this section, the person is again convicted of a recordable offence, the material may be retained indefinitely.

(5A) In subsection (5), the reference to a recordable offence includes an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence if done in England and Wales.

(6) In this section, "relevant custodial sentence" means any of the following—

(a) a custodial sentence within the meaning of section 76 of the Powers of Criminal Courts (Sentencing) Act 2000 or section 222 of the Sentencing Code;
(b) a sentence of a period of detention and training (excluding any period of supervision) which a person is liable to serve under an order under section 211 of the Armed Forces Act 2006 or a secure training order.

Section 63L – Retention of section 63D material: persons given a penalty notice

(1) This section applies to section 63D material which—

(a) relates to a person who is given a penalty notice under section 2 of the Criminal Justice and Police Act 2001 and in respect of whom no proceedings are brought for the offence to which the notice relates, and
(b) was taken (or, in the case of a DNA profile, derived from a sample taken) from the person in connection with the investigation of the offence to which the notice relates.

(2) The material may be retained—

(a) in the case of fingerprints, for a period of 2 years beginning with the date on which the fingerprints were taken,
(b) in the case of a DNA profile, for a period of 2 years beginning with—

(i) the date on which the DNA sample from which the profile was derived was taken, or
(ii) if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken.

Section 63M – Retention of section 63D material for purposes of national security

(1) Section 63D material may be retained for as long as a national security determination made by a chief officer of police has effect in relation to it.

(2) A national security determination is made if a chief officer of police determines that it is necessary for any section 63D material to be retained for the purposes of national security.

(3) A national security determination—

(a) must be made in writing,
(b) has effect for a maximum of 5 years beginning with the date on which it is made, and
(c) may be renewed.

Section 63N – Retention of section 63D material given voluntarily

(1) This section applies to the following section 63D material—

(a) fingerprints taken with the consent of the person from whom they were taken, and
(b) a DNA profile derived from a DNA sample taken with the consent of the person from whom the sample was taken.

(2) Material to which this section applies may be retained until it has fulfilled the purpose for which it was taken or derived.

(3) Material to which this section applies which relates to—

(a) a person who is convicted of a recordable offence, o
(b) a person who has previously been convicted of a recordable offence (other than a person who has only one exempt conviction), may be retained indefinitely.

(4) For the purposes of subsection (3)(b), a conviction is exempt if it is in respect of a recordable offence, other than a qualifying offence, committed when the person is aged under 18.

(5) The reference to a recordable offence in subsection (3)(a) includes an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence if done in England and Wales.

(6) The reference to a recordable offence in subsections (3)(b) and (4), and the reference to a qualifying offence in subsection (4), includes an offence under the law of a country or territory outside England and Wales where the act constituting the offence would constitute a recordable offence or (as the case may be) a qualifying offence if done in England and Wales (whether or not it constituted such an offence when the person was convicted).

Section 63O – Retention of section 63D material with consent

(1) This section applies to the following material—

(a) fingerprints (other than fingerprints taken under section 61(6A)) to which section 63D applies, and
(b) a DNA profile to which section 63D applies.

(2) If the person to whom the material relates consents to material to which this section applies being retained, the material may be retained for as long as that person consents to it being retained.

(3) Consent given under this section—

(a) must be in writing, and
(b) can be withdrawn at any time.

Section 63R – Destruction of samples

(1) This section applies to samples—

(a) taken from a person under any power conferred by this Part of this Act, or
(b) taken by the police, with the consent of the person from whom they were taken, in connection with the investigation of an offence by the police.

(2) Samples to which this section applies must be destroyed if it appears to the responsible chief officer of police that—

(a) the taking of the samples was unlawful, or
(b) the samples were taken from a person in connection with that person's arrest and the arrest was unlawful or based on mistaken identity.

(3) Subject to this, the rule in subsection (4) or (as the case may be) (5) applies.

(4) A DNA sample to which this section applies must be destroyed—

(a) as soon as a DNA profile has been derived from the sample, or
(b) if sooner, before the end of the period of 6 months beginning with the date on which the sample was taken.

(5) Any other sample to which this section applies must be destroyed before the end of the period of 6 months beginning with the date on which it was taken.

(6) The responsible chief officer of police may apply to a District Judge (Magistrates' Courts) for an order to retain a sample to which this section applies beyond the date on which the sample would otherwise be required to be destroyed by virtue of subsection (4) or (5) if—

(a) the sample was taken from a person in connection with the investigation of a qualifying offence, and
(b) the responsible chief officer of police considers that the condition in subsection (7) is met.

(7) The condition is that, having regard to the nature and complexity of other material that is evidence in relation to the offence, the sample is likely to be needed in any proceedings for the offence for the purposes of—

(a) disclosure to, or use by, a defendant, or
(b) responding to any challenge by a defendant in respect of the admissibility of material that is evidence on which the prosecution proposes to rely.

(8) An application under subsection (6) must be made before the date on which the sample would otherwise be required to be destroyed by virtue of subsection (4) or (5).

(9) If, on an application made by the responsible chief officer of police under subsection (6), the District Judge (Magistrates' Courts) is satisfied that the condition in subsection (7) is met, the District Judge may make an order under this subsection which—

> (a) allows the sample to be retained for a period of 12 months beginning with the date on which the sample would otherwise be required to be destroyed by virtue of subsection (4) or (5), and
> (b) may be renewed (on one or more occasions) for a further period of not more than 12 months from the end of the period when the order would otherwise cease to have effect.

(10) An application for an order under subsection (9) (other than an application for renewal)—

> (a) may be made without notice of the application having been given to the person from whom the sample was taken, and
> (b) may be heard and determined in private in the absence of that person.

(11) A sample retained by virtue of an order under subsection (9) must not be used other than for the purposes of any proceedings for the offence in connection with which the sample was taken.

(12) A sample that ceases to be retained by virtue of an order under subsection (9) must be destroyed.

(13) Nothing in this section prevents a speculative search, in relation to samples to which this section applies, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

Section 64A – Photographing of suspects etc.

(1) A person who is detained at a police station may be photographed—

(a) with the appropriate consent; or
(b) if the appropriate consent is withheld or it is not practicable to obtain it, without it.

(1A) A person falling within subsection (1B) below may, on the occasion of the relevant event referred to in subsection (1B), be photographed elsewhere than at a police station—

(a) with the appropriate consent; or
(b) if the appropriate consent is withheld or it is not practicable to obtain it, without it.

(1B) A person falls within this subsection if he has been—

(a) arrested by a constable for an offence;
(b) taken into custody by a constable after being arrested for an offence by a person other than a constable;
(c) made subject to a requirement to wait with a community support officer or a community support volunteer under paragraph 7 of Schedule 3B to the Police Reform Act 2002 ("the 2002 Act");
(ca) given a direction by a constable under section 35 of the Anti-social Behaviour, Crime and Policing Act 2014;
(d) given a penalty notice by a constable under Chapter 1 of Part 1 of the Criminal Justice and Police Act 2001, a penalty notice by a constable under section 444A of the Education Act 1996, or a fixed penalty notice by a constable in uniform under section 54 of the Road Traffic Offenders Act 1988;
(e) given a fixed penalty notice by a community support officer or community support volunteer who is authorised to give the notice by virtue of his or her designation under section 38 of the Police Reform Act 2002;
(f) given a notice in relation to a relevant fixed penalty offence (within the meaning of paragraph 1 of Schedule 5 to the 2002 Act) by an accredited person by virtue of accreditation specifying that that paragraph applies to him; or
(g) given a notice in relation to a relevant fixed penalty offence

(within the meaning of Schedule 5A to the 2002 Act) by an accredited inspector by virtue of accreditation specifying that paragraph 1 of Schedule 5A to the 2002 Act applies to him.

(2) A person proposing to take a photograph of any person under this section—

(a) may, for the purpose of doing so, require the removal of any item or substance worn on or over the whole or any part of the head or face of the person to be photographed; and
(b) if the requirement is not complied with, may remove the item or substance himself.

(3) Where a photograph may be taken under this section, the only persons entitled to take the photograph are constables.

(4) A photograph taken under this section—

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

(5) In subsection (4)—

(a) the reference to crime includes a reference to any conduct which—

(i) constitutes one or more criminal offences (whether under the law of a part of the United Kingdom or of a country or territory outside the United Kingdom); or
(ii) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences; and

(b) the references to an investigation and to a prosecution include references, respectively, to any investigation outside the United Kingdom of any crime or suspected crime and to a prosecution brought in respect of any crime in a country or territory outside the United Kingdom; and

(c) "sentence" includes any order made by a court in England and Wales when dealing with an offender in respect of his offence.

(6) References in this section to taking a photograph include references to using any process by means of which a visual image may be produced; and references to photographing a person shall be construed accordingly.

(6A) In this section, a "photograph" includes a moving image, and corresponding expressions shall be construed accordingly.

(7) Nothing in this section applies to a person arrested under an extradition arrest power.

Section 65 – Part V—supplementary

(1) In this Part of this Act—

"analysis", in relation to a skin impression, includes comparison and matching;

"appropriate consent" means —

(a) in relation to a person who [has attained the age of 18 years, the consent of that person;
(b) in relation to a person who has not attained that age but has attained the age of 14 years, the consent of that person and his parent or guardian; and
(c) in relation to a person who has not attained the age of 14 years, the consent of his parent or guardian;

"DNA profile" means any information derived from a DNA sample;

"DNA sample" means any material that has come from a human body and consists of or includes human cells;

"extradition arrest power" means any of the following—

(a) a Part 1 warrant (within the meaning given by the

Extradition Act 2003) in respect of which a certificate under section 2 of that Act has been issued;
(b) section 5 of that Act;
(c) a warrant issued under section 71 of that Act;
(d) a provisional warrant (within the meaning given by that Act);
(e) section 74A of that Act;

"fingerprints", in relation to any person, means a record (in any form and produced by any method) of the skin pattern and other physical characteristics or features of–

(a) any of that person's fingers; or
(b) either of his palms;

"intimate sample" means—

(a) a sample of blood, semen or any other tissue fluid, urine or pubic hair;
(b) a dental impression;
(c) a swab taken from any part of a person's genitals (including pubic hair) or from a person's body orifice other than the mouth;

"intimate search" means a search which consists of the physical examination of a person's body orifices other than the mouth;

"non-intimate sample" means—

(a) a sample of hair other than pubic hair;
(b) a sample taken from a nail on from under a nail;
(c) a swab taken from any part of a person's body other than a part from which a swab taken would be an intimate sample;
(d) saliva;
(e) a skin impression;

"offence", in relation to any country or territory outside England and Wales, includes an act punishable under the law of that country or territory, however it is described;

"registered dentist" has the same meaning as in the Dentists Act 1984;

"skin impression" , in relation to any person, means any record (other than a fingerprint) which is a record (in any form and produced by any method) of the skin pattern and other physical characteristics or features of the whole or any part of his foot or of any other part of his body;

"registered health care professional" means a person (other than a medical practitioner) who is—

(a) a registered nurse; or
(b) a registered member of a health care profession which is designated for the purposes of this paragraph by an order made by the Secretary of State;

"the responsible chief officer of police", in relation to material to which section 63D or 63R applies, means the chief officer of police for the police area—

(a) in which the material concerned was taken, or
(b) in the case of a DNA profile, in which the sample from which the DNA profile was derived was taken;

"section 63D material" means fingerprints or DNA profiles to which section 63D applies;

"speculative search", in relation to a person's fingerprints or samples, means such a check against other fingerprints or samples or against information derived from other samples as is referred to in section 63A(1) above;

"sufficient" and "insufficient", in relation to a sample, means (subject to subsection (2) below) sufficient or insufficient (in point of quantity or quality) for the purpose of enabling information to be produced by the means of analysis used or to be used in relation to the sample.

"the terrorism provisions" means section 41 of the Terrorism Act 2000, and any provision of Schedule 7 to that Act conferring a power of detention; and

"terrorism" has the meaning given in section 1 of that Act.

"terrorist investigation" has the meaning given by section 32 of that Act;

(1A) A health care profession is any profession mentioned in section 60(2) of the Health Act 1999 other than the profession of practising medicine and the profession of nursing.

(1B) An order under subsection (1) shall be made by statutory instrument and shall be subject to annulment in pursuance of a resolution of either House of Parliament.

(2) References in this Part of this Act to a sample's proving insufficient include references to where, as a consequence of–

(a) the loss, destruction or contamination of the whole or any part of the sample,
(b) any damage to the whole or a part of the sample, or
(c) the use of the whole or a part of the sample for an analysis which produced no results or which produced results some or all of which must be regarded, in the circumstances, as unreliable, the sample has become unavailable or insufficient for the purpose of enabling information, or information of a particular description, to be obtained by means of analysis of the sample.

(2A) In subsection (2), the reference to the destruction of a sample does not include a reference to the destruction of a sample under section 63R (requirement to destroy samples).

(2B) Any reference in sections 63F, 63H, 63P or 63U to a person being charged with an offence includes a reference to a person being informed that the person will be reported for an offence.

(3) For the purposes of this Part, a person has in particular been convicted of an offence under the law of a country or territory outside England and Wales if—

(a) a court exercising jurisdiction under the law of that country or territory has made in respect of such an offence a finding equivalent to a finding that the person is not guilty by reason of insanity; or

(b) such a court has made in respect of such an offence a finding equivalent to a finding that the person is under a disability and did the act charged against him in respect of the offence.

Section 65A – "Qualifying offence"

(1) In this Part, "qualifying offence" means—

(a) an offence specified in subsection (2) below, or
(b) an ancillary offence relating to such an offence.

(2) The offences referred to in subsection (1)(a) above are—

(a) murder;
(b) manslaughter;
(c) false imprisonment;
(d) kidnapping;
(da) an offence of indecent exposure;
(db) an offence under section 4 of the Vagrancy Act 1824, committed by a person by wilfully, openly, lewdly, and obscenely exposing his person with intent to insult any female;
(dc) an offence under section 28 of the Town Police Clauses Act 1847, committed by a person by wilfully and indecently exposing his person;
(e) an offence under section 4, 16, 18, 20 to 24 or 47 of the Offences Against the Person Act 1861;
(f) an offence under section 2 or 3 of the Explosive Substances Act 1883;
(fa) an offence under section 1 of the Infant Life (Preservation) Act 1929;
(g) an offence under section 1 of the Children and Young Persons Act 1933;
(ga) an offence under section 1 of the Infanticide Act 1938;
(gb) an offence under section 12 or 13 of the Sexual Offences Act 1956, other than an offence committed by a person where the other person involved in the conduct constituting the offence consented to it and was aged 16 or over;
(gc) an offence under any other section of that Act, other than sections 18 and 32;
(gd) an offence under section 128 of the Mental Health Act 1959;

(ge) an offence under section 1 of the Indecency with Children Act 196;
(h) an offence under section 4(1) of the Criminal Law Act 1967 committed in relation to murder;
(ha) an offence under section 5 of the Sexual Offences Act 1967;
(i) an offence under sections 16 to 18 of the Firearms Act 1968;
(j) an offence under [section 8, 9 or 10 of the Theft Act 1968 or an offence under section 12A of that Act involving an accident which caused a person's death;
(ja) an offence under section 1(1) of the Genocide Act 1969;
(k) an offence under section 1 of the Criminal Damage Act 1971 required to be charged as arson;
(ka) an offence under section 54 of the Criminal Law Act 1977;
(l) an offence under section 1 of the Protection of Children Act 1978;
(m) an offence under section 1 of the Aviation Security Act 1982;
(n) an offence under section 2 of the Child Abduction Act 1984;
(na) an offence under section 1 of the Prohibition of Female Circumcision Act 1985;
(nb) an offence under section 1 of the Public Order Act 1986;
(o) an offence under section 9 of the Aviation and Maritime Security Act 1990;
(oa) an offence under section 3 of the Sexual Offences (Amendment) Act 2000;
(ob) an offence under section 51 of the International Criminal Court Act 2001;
(oc) an offence under section 1, 2 or 3 of the Female Genital Mutilation Act 2003;
(p) an offence under any of [sections 1 to 19, 25, 26, 30 to 41, 47 to 50, 52, 53, 57 to 59A, 61 to 67, 69 and 70 of the Sexual Offences Act 2003;
(q) an offence under section 5 of the Domestic Violence, Crime and Victims Act 2004;
(r) an offence for the time being listed in section 41(1) of the Counter-Terrorism Act 2008;
(s) an offence under section 2 of the Modern Slavery Act 2015 (human trafficking) ;
(t) an offence under paragraph 1 of Schedule 4 to the Space Industry Act 2018.

(3) The Secretary of State may by order made by statutory instrument amend subsection (2) above.

(4) A statutory instrument containing an order under subsection (3) above shall not be made unless a draft of the instrument has been laid before, and approved by resolution of, each House of Parliament.

(5) In subsection (1)(b) above "ancillary offence", in relation to an offence, means—

(a) aiding, abetting, counselling or procuring the commission of the offence;
(b) an offence under Part 2 of the Serious Crime Act 2007 (encouraging or assisting crime) in relation to the offence (including, in relation to times before the commencement of that Part, an offence of incitement);
(c) attempting or conspiring to commit the offence.

Terrorism Act 2000

Schedule 7 – Port and Border Controls

Paragraph 2

(1) An examining officer may question a person to whom this paragraph applies for the purpose of determining whether he appears to be a person falling within section 40(1)(b).

(2) This paragraph applies to a person if—

(a) he is at a port or in the border area, and
(b) the examining officer believes that the person's presence at the port or in the area is connected with his entering or leaving Great Britain or Northern Ireland or his travelling by air within Great Britain or within Northern Ireland.

(3) This paragraph also applies to a person on a ship or aircraft which has arrived at any place in Great Britain or Northern Ireland (whether from within or outside Great Britain or Northern Ireland).

(4) An examining officer may exercise his powers under this paragraph whether or not he has grounds for suspecting that a person falls within section 40(1)(b).

[...]

Paragraph 6

(1) For the purposes of exercising a power under paragraph 2 or 3 an examining officer may—

(a) stop a person or vehicle;
(b) detain a person.

(2) For the purpose of detaining a person under this paragraph, an examining officer may authorise the person's removal from a ship, aircraft or vehicle.

(3) Where a person is detained under this paragraph the provisions of Parts 1 and 1A of Schedule 8 (treatment and review of detention) shall apply.

Schedule 8 – Detention

Paragraph 2 — Identification

(1) An authorised person may take any steps which are reasonably necessary for–

(a) photographing the detained person,
(b) measuring him, or
(c) identifying him.

(2) In sub-paragraph (1) "authorised person" means any of the following–

(a) a constable,
(b) a prison officer,
(c) a person authorised by the Secretary of State, and
(d) in the case of a person detained under Schedule 7, an examining officer.

(3) This paragraph does not confer the power to take–

(a) fingerprints, non-intimate samples or intimate samples (within the meaning given by paragraph 15 below), [...].

Paragraph 10

[...]

(2) Fingerprints may be taken from the detained person only if they are taken by a constable–

(a) with the appropriate consent given in writing, or
(b) without that consent under sub-paragraph (4).

[...]

(4) Fingerprints or a non-intimate sample may be taken from the detained person without the appropriate consent only if–

(a) he is detained at a police station and a police officer of at least the rank of superintendent authorises the fingerprints or sample to be taken, or
(b) he has been convicted of a recordable offence and, where a non-intimate sample is to be taken, he was convicted of the offence on or after 10th April 1995 (or 29th July 1996 where the non-intimate sample is to be taken in Northern Ireland).

[...]

(6) Subject to sub-paragraph (6A) an officer may give an authorisation under sub-paragraph (4)(a) or (5)(c) only if–

(a) in the case of a person detained under section 41, the officer reasonably suspects that the person has been involved in an offence under any of the provisions mentioned in section 40(1)(a), and the officer reasonably believes that the fingerprints or sample will tend to confirm or disprove his involvement, or
(b) in any case in which an authorisation under that sub-paragraph may be given, the officer is satisfied that the taking of the fingerprints or sample from the person is necessary in order to assist in determining whether he falls within section 40(1)(b).

(6A) An officer may also give an authorisation under sub-paragraph (4)(a) for the taking of fingerprints if—

(a) he is satisfied that the fingerprints of the detained person will facilitate the ascertainment of that person's identity; and
(b) that person has refused to identify himself or the officer has reasonable grounds for suspecting that that person is not who he claims to be.

Paragraph 20A

(1) This paragraph applies to—

(a) fingerprints taken under paragraph 10,
(b) a DNA profile derived from a DNA sample taken under paragraph 10 or 12,
(c) relevant physical data taken or provided by virtue of paragraph 20, and
(d) a DNA profile derived from a DNA sample taken by virtue of paragraph 20.

(2) Fingerprints, relevant physical data and DNA profiles to which this paragraph applies ("paragraph 20A material") must be destroyed if it appears to the responsible chief officer of police that—

(a) the taking or providing of the material or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful, or
(b) the material was taken or provided, or (in the case of a DNA profile) was derived from a sample taken, from a person in connection with that person's arrest under section 41 and the arrest was unlawful or based on mistaken identity.

(3) In any other case, paragraph 20A material must be destroyed unless it is retained under any power conferred by paragraphs 20B to 20E.

(4) Paragraph 20A material which ceases to be retained under a power mentioned in sub-paragraph (3) may continue to be retained under any other such power which applies to it.

(5) Nothing in this paragraph prevents a relevant search, in relation

to paragraph 20A material, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

(6) For the purposes of sub-paragraph (5), "a relevant search" is a search carried out for the purpose of checking the material against—

(a) other fingerprints or samples taken under paragraph 10 or 12 or a DNA profile derived from such a sample,

[...]

(d) material to which section 18 of the Counter-Terrorism Act 2008 applies,
(e) any of the fingerprints, data or samples obtained under paragraph 1 or 4 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011, or information derived from such samples,
(ea) any of the fingerprints, data or samples obtained under or by virtue of paragraph 34 or 42 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019, or information derived from such samples,
(f) any of the fingerprints, samples and information mentioned in section 63A(1)(a) and (b) of the Police and Criminal Evidence Act 1984 (checking of fingerprints and samples), [...]

Paragraph 20B

(1) This paragraph applies to paragraph 20A material relating to a person who is detained under section 41.

(2) In the case of a person who has previously been convicted of a recordable offence (other than a single exempt conviction), or an offence in Scotland which is punishable by imprisonment, or is so convicted before the end of the period within which the material may be retained by virtue of this paragraph, the material may be retained indefinitely.

(2A) In sub-paragraph (2) —

(a) the reference to a recordable offence includes an offence under the law of a country or territory outside the United Kingdom where the act constituting the offence would constitute—

(i) a recordable offence under the law of England and Wales if done there, [...]

(3) In the case of a person who has no previous convictions, or only one exempt conviction, the material may be retained until the end of the retention period specified in sub-paragraph (4).

(4) The retention period is—

(a) in the case of fingerprints or relevant physical data, the period of 3 years beginning with the date on which the fingerprints or relevant physical data were taken or provided, and
(b) in the case of a DNA profile, the period of 3 years beginning with the date on which the DNA sample from which the profile was derived was taken (or, if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken).

(5) The responsible chief officer of police or a specified chief officer of police may apply to a relevant court for an order extending the retention period.

(6) An application for an order under sub-paragraph (5) must be made within the period of 3 months ending on the last day of the retention period.

(7) An order under sub-paragraph (5) may extend the retention period by a period which—

(a) begins with the date on which the material would otherwise be required to be destroyed under this paragraph, and
(b) ends with the end of the period of 2 years beginning with that date.

(8) The following persons may appeal to the relevant appeal court against an order under sub-paragraph (5), or a refusal to make such an order—

(a) the responsible chief officer of police;
(b) a specified chief officer of police;
(c) the person from whom the material was taken.

[...]

(10) In this paragraph—

"relevant court" means—

(a) in England and Wales, a District Judge (Magistrates' Courts),

[...]

"the relevant appeal court" means—

(a) in England and Wales, the Crown Court,

[...]

"a specified chief officer of police" means—

(a) in England and Wales and Northern Ireland—

(i) the chief officer of the police force of the area in which the person from whom the material was taken resides, or
(ii) a chief officer of police who believes that the person is in, or is intending to come to, the chief officer's police area, [...]

Paragraph 20C

(1) This paragraph applies to paragraph 20A material relating to a person who is detained under Schedule 7.

(2) In the case of a person who has previously been convicted of a recordable offence (other than a single exempt conviction), or an offence in Scotland which is punishable by imprisonment, or is so convicted before the end of the period within which the material may be retained by virtue of this paragraph, the material may be retained indefinitely.

(2A) In sub-paragraph (2) —

(a) the reference to a recordable offence includes an offence under the law of a country or territory outside the United Kingdom where the act constituting the offence would constitute—

(i) a recordable offence under the law of England and Wales if done there, [...]

(3) In the case of a person who has no previous convictions, or only one exempt conviction, the material may be retained until the end of the retention period specified in sub-paragraph (4).

(4) The retention period is—

(a) in the case of fingerprints or relevant physical data, the period of 6 months beginning with the date on which the fingerprints or relevant physical data were taken or provided, and
(b) in the case of a DNA profile, the period of 6 months beginning with the date on which the DNA sample from which the profile was derived was taken (or, if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken).

Paragraph 20D

(1) For the purposes of paragraphs 20B and 20C, a person is to be treated as having been convicted of an offence if—

(a) in relation to a recordable offence in England and Wales or Northern Ireland—

(i) the person has been given a caution in respect of the offence which, at the time of the caution, the person has admitted,
(ii) the person has been found not guilty of the offence by reason of insanity,
(iii) the person has been found to be under a disability and to have done the act charged in respect of the offence, or
(iv) the person has been warned or reprimanded under section 65 of the Crime and Disorder Act 1998 for the offence,

[...]

(2) Paragraphs 20B and 20C and this paragraph, so far as they relate to persons convicted of an offence, have effect despite anything in the Rehabilitation of Offenders Act 1974.

(3) But a person is not to be treated as having been convicted of an offence if that conviction is a disregarded conviction or caution by virtue of section 92 of the Protection of Freedoms Act 2012.

(4) For the purposes of paragraphs 20B and 20C—

(a) a person has no previous convictions if the person has not previously been convicted—

(i) in England and Wales or Northern Ireland of a recordable offence, [...]
(ii) [...] and

(b) if the person has previously been convicted of a recordable offence in England and Wales or Northern Ireland, the conviction is exempt if it is in respect of a recordable offence, other than a qualifying offence, committed when the person was aged under 18.

(5) In sub-paragraph (4), "qualifying offence" has—

(a) in relation to a conviction in respect of a recordable offence committed in England and Wales, the meaning given by section 65A of the Police and Criminal Evidence Act 1984, [...

(5A) For the purposes of sub-paragraph (4)—

(a) a person is to be treated as having previously been convicted in England and Wales of a recordable offence if —

(i) the person has previously been convicted of an offence under the law of a country or territory outside the United Kingdom, and
(ii) the act constituting the offence would constitute a recordable offence under the law of England and Wales if done there (whether or not it constituted such an offence when the person was convicted);

[...]

(d) the reference in sub-paragraph (4)(b) to a qualifying offence includes a reference to an offence under the law of a country or territory outside the United Kingdom where the act constituting the offence would constitute a qualifying offence under the law of England and Wales if done there [...].

(5B) For the purposes of paragraphs 20B and 20C and this paragraph—

(a) offence, in relation to any country or territory outside the United Kingdom, includes an act punishable under the law of that country or territory, however it is described;
(b) a person has in particular been convicted of an offence under the law of a country or territory outside the United Kingdom if—

(i) a court exercising jurisdiction under the law of that country or territory has made in respect of such an offence a finding equivalent to a finding that the person is not guilty by reason of insanity, or
(ii) such a court has made in respect of such an offence a finding equivalent to a finding that the person is under a disability and did the act charged against the person in respect of the offence.

(6) If a person is convicted of more than one offence arising out of a single course of action, those convictions are to be treated as a

single conviction for the purposes of calculating under paragraph 20B or 20C whether the person has been convicted of only one offence.

(7) Nothing in paragraph 20B or 20C prevents the start of a new retention period in relation to paragraph 20A material if a person is detained again under section 41 or (as the case may be) Schedule 7 when an existing retention period (whether or not extended) is still in force in relation to that material.

Paragraph 20E

(1) Paragraph 20A material may be retained for as long as a national security determination made by a chief officer of police has effect in relation to it.

(2) A national security determination is made if a chief officer of police determines that it is necessary for any paragraph 20A material to be retained for the purposes of national security.

(3) A national security determination—

(a) must be made in writing,
(b) has effect for a maximum of 5 years beginning with the date on which the determination is made, and
(c) may be renewed.

(4) In this paragraph "chief officer of police" means—

(a) a chief officer of police of a police force in England and Wales, [...]

Counter-Terrorism Act 2008

Section 18 – Destruction of national security material not subject to existing statutory restrictions

(1) This section applies to fingerprints, DNA samples and DNA profiles that—

(a) are held for the purposes of national security by a law enforcement authority under the law of England and Wales or Northern Ireland, and
(b) are not held subject to existing statutory restrictions.

(2) Material to which this section applies ("section 18 material") must be destroyed if it appears to the responsible officer that the condition in subsection (3) is not met.

(3) The condition is that the material has been—

(a) obtained by the law enforcement authority pursuant to an authorisation under Part 3 of the Police Act 1997 (authorisation of action in respect of property),
(b) obtained by the law enforcement authority in the course of surveillance, or use of a covert human intelligence source, authorised under Part 2 of the Regulation of Investigatory Powers Act 2000,
(c) supplied to the law enforcement authority by another law enforcement authority, or
(d) otherwise lawfully obtained or acquired by the law enforcement authority for any of the purposes mentioned in section 18D(1).

(4) In any other case, section 18 material must be destroyed unless it is retained by the law enforcement authority under any power conferred by section 18A or 18B, but this is subject to subsection (5).

(5) A DNA sample to which this section applies must be destroyed—

(a) as soon as a DNA profile has been derived from the sample, or
(b) if sooner, before the end of the period of 6 months beginning with the date on which it was taken.

(6) Section 18 material which ceases to be retained under a power mentioned in subsection (4) may continue to be retained under any other such power which applies to it.

(7) Nothing in this section prevents section 18 material from being checked against other fingerprints, DNA samples or DNA profiles held by a law enforcement authority within such time as may

reasonably be required for the check, if the responsible officer considers the check to be desirable.

(8) For the purposes of subsection (1), the following are "existing statutory restrictions"—

(a) paragraph 18(2) of Schedule 2 to the Immigration Act 1971;
(b) sections 22, 63A and 63D to 63U of the Police and Criminal Evidence Act 1984 and any corresponding provision in an order under section 113 of that Act;

[...]

(d) section 2(2) of the Security Service Act 1989;
(e) section 2(2) of the Intelligence Services Act 1994;
(f) paragraphs 20(3) and 20A to 20J of Schedule 8 to the Terrorism Act 2000;
(g) section 56 of the Criminal Justice and Police Act 2001;
(h) paragraph 8 of Schedule 4 to the International Criminal Court Act 2001;
(i) sections 73, 83, 87, 88 and 89 of the Armed Forces Act 2006 and any provision relating to the retention of material in an order made under section 74, 93 or 323 of that Act;
(j) paragraphs 5 to 14 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011;
(k) paragraphs 43 to 51 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019.

Section 18A – Retention of material: general

[...]

(2) The retention period is—

(a) in the case of fingerprints, the period of 3 years beginning with the date on which the fingerprints were taken, and
s(b) in the case of a DNA profile, the period of 3 years beginning with the date on which the DNA sample from which the profile was derived was taken (or, if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken).

Terrorism Prevention and Investigation Measures Act 2011

Schedule 6

Paragraph 6 – Requirement to destroy material

(1) This paragraph applies to—

(a) fingerprints taken under paragraph 1,
(b) a DNA profile derived from a DNA sample taken under that paragraph,
(c) relevant physical data taken or provided under paragraph 4,
(d) a DNA profile derived from a DNA sample taken under that paragraph.

(2) Fingerprints, relevant physical data and DNA profiles to which this paragraph applies ("paragraph 6 material") must be destroyed if it appears to the responsible chief officer of police that the taking or providing of the material or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful.

(3) In any other case, paragraph 6 material must be destroyed unless it is retained under a power conferred by paragraph 8, 9 or 11.

(4) Paragraph 6 material that ceases to be retained under a power mentioned in sub-paragraph (3) may continue to be retained under any other such power that applies to it.

(5) Nothing in this paragraph prevents a relevant search from being carried out, in relation to paragraph 6 material, within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

Paragraph 7 – Requirement to destroy material

(1) If fingerprints or relevant physical data are required by paragraph 6 to be destroyed, any copies of the fingerprints or data held by a police force must also be destroyed.

(2) If a DNA profile is required by that paragraph to be destroyed, no copy may be retained by a police force except in a form which does

not include information which identifies the individual to whom the DNA profile relates.

Paragraph 8 – Retention of paragraph 6 material

(1) This paragraph applies to paragraph 6 material taken from, or provided by, an individual who has no previous convictions or (in the case of England and Wales or Northern Ireland) only one exempt conviction.

(2) The material may be retained until the end of the period of 6 months beginning with the date on which the TPIM notice that was in force when the material was taken ceases to be in force (subject to sub-paragraphs (3) and (4)).

(3) If, before the end of that period, the TPIM notice is quashed by the court under this Act, the material may be retained only until there is no possibility of an appeal against—

(a) the decision to quash the notice, or
(b) any decision made on an appeal against that decision.

(4) If, after a TPIM notice is quashed or otherwise ceases to be in force, measures are imposed on the individual (whether by the revival of a TPIM notice or the imposition of a new TPIM notice)—

(a) within the period for which material in relation to the individual is retained by virtue of sub-paragraph (2), or
(b) within, or immediately after the end of, the period for which such material is retained by virtue of sub-paragraph (3), sub-paragraphs (2) and (3) apply again for the purposes of the retention of that material (taking references to the TPIM notice as references to the revived or new TPIM notice).

(5) In determining whether there is no further possibility of an appeal against a decision of the kind mentioned in sub-paragraph (3), any power to extend the time for giving notice of application for leave to appeal, or for applying for leave to appeal, must be ignored.

Paragraph 9 – Retention of paragraph 6 material

(1) This paragraph applies to paragraph 6 material taken from, or provided by, an individual—

(a) who has been convicted of a recordable offence (other than a single exempt conviction) or of an offence in Scotland which is punishable by imprisonment, or
(b) who is so convicted before the end of the period within which the material may be retained by virtue of paragraph 8.

(2) The material may be retained indefinitely.

Paragraph 10 – Retention of paragraph 6 material

(1) For the purposes of paragraphs 8 and 9 an individual is to be treated as having been convicted of an offence if—

(a) in relation to a recordable offence in England and Wales or Northern Ireland—

(i) the individual has been given a caution in respect of the offence which, at the time of the caution, the individual has admitted,
(ii) the individual has been found not guilty of the offence by reason of insanity, or
(iii) the individual has been found to be under a disability and to have done the act charged in respect of the offence,
[...]

(2) Paragraphs 8, 9 and this paragraph, so far as they relate to individuals convicted of an offence, have effect despite anything in the Rehabilitation of Offenders Act 1974.

(2A) But a person is not to be treated as having been convicted of an offence if that conviction is a disregarded conviction or caution by virtue of section 92 of the Protection of Freedoms Act 2012.

(3) For the purposes of paragraphs 8 and 9—

(a) an individual has no previous convictions if the individual has not previously been convicted—

(i) in England and Wales or Northern Ireland of a recordable offence, [...]
(ii) [...], and

(b) if the individual has previously been convicted of a recordable offence in England and Wales or Northern Ireland, the conviction is exempt if it is in respect of a recordable offence, other than a qualifying offence, committed when the individual was aged under 18.

(4) In sub-paragraph (3) "qualifying offence" has—

(a) in relation to a conviction in respect of a recordable offence committed in England and Wales, the meaning given by section 65A of the Police and Criminal Evidence Act 1984 [...].

(5) If an individual is convicted of more than one offence arising out of a single course of action, those convictions are to be treated as a single conviction for the purposes of calculating under paragraph 8 or 9 whether the individual has been convicted of one offence.

Counter-Terrorism and Border Security Act 2019

Schedule 3 – Border security

Paragraph 34

(1) This paragraph applies where a detainee is detained in England, Wales or Northern Ireland.

(2) Fingerprints may be taken from the detainee only if they are taken by a constable—

(a) with the appropriate consent given in writing, or
(b) without that consent under sub-paragraph (4).

(3) A non-intimate sample may be taken from the detainee only if it is taken by a constable—

(a) with the appropriate consent given in writing, or
(b) without that consent under sub-paragraph (4).

(4) Fingerprints or a non-intimate sample may be taken from the detainee without the appropriate consent only if—

(a) the detainee is detained at a police station and a police officer of at least the rank of superintendent authorises the fingerprints or sample to be taken, or
(b) the detainee has been convicted of a recordable offence and, where a non-intimate sample is to be taken, was convicted of the offence on or after 10th April 1995 (or 29th July 1996 where the non-intimate sample is to be taken in Northern Ireland).

(5) An officer may give an authorisation under sub-paragraph (4)(a) only if—

(a) in the case of the taking of fingerprints or samples, condition 1 is met, or
(b) in the case of the taking of fingerprints, condition 2 is met.

(6) Condition 1 is met if the officer is satisfied that it is necessary for the fingerprints or sample to be taken in order to assist in determining whether the detainee is or has been engaged in hostile activity.

(7) Condition 2 is met if—

(a) the officer is satisfied that the fingerprints of the detainee will facilitate the ascertainment of the detainee's identity, and
(b) the detainee has refused to identify himself or herself or the officer has reasonable grounds for suspecting that the detainee is not who the detainee claims to be.

(8) In this paragraph references to ascertaining a person's identity include references to showing that the person is not a particular person.

(9) If an authorisation under sub-paragraph (4)(a) is given orally, the person giving it must confirm it in writing as soon as is reasonably practicable.

Paragraph 35

(1) Before fingerprints or a sample are taken from a person under paragraph 34, the person must be informed—

(a) that the fingerprints or sample may be used for the purposes of—

(i) a relevant search, as defined by paragraph 43(6),
(ii) section 63A(1) of the Police and Criminal Evidence Act 1984, or
(iii) [...], and

(b) where the fingerprints or sample are to be taken under paragraph 34(2)(a), (3)(a) or (4)(b), of the reason for taking the fingerprints or sample.

(2) Before fingerprints or a sample are taken from a detainee upon an authorisation given under paragraph 34(4)(a), the detainee must be informed—

(a) that the authorisation has been given,
(b) of the grounds upon which it has been given, and
(c) where relevant, of the nature of the offence in which it is suspected that the detainee has been involved.

(3) After fingerprints or a sample are taken under paragraph 34, any of the following which apply must be recorded as soon as reasonably practicable—

(a) the fact that the person has been informed in accordance with sub-paragraphs (1) and (2),
(b) the reason referred to in sub-paragraph (1)(b),
(c) the authorisation given under paragraph 34(4)(a),
(d) the grounds upon which that authorisation has been given, and
(e) the fact that the appropriate consent has been given.

(4) Where a sample of hair is to be taken under paragraph 34, the sample may be taken either by cutting hairs or by plucking hairs with their roots so long as no more are plucked than the person taking the sample reasonably considers to be necessary for a sufficient sample.

Paragraph 36

(1) In the application of paragraphs 26, 34 and 35 in relation to a person detained in England or Wales, the following expressions have the meaning given by section 65 of the Police and Criminal Evidence Act 1984—

(a) "appropriate consent",
(b) "fingerprints",
(c) "intimate sample",
(d) "non-intimate sample", and
(e) "sufficient".

(2) In the application of section 65(2A) of the Police and Criminal Evidence Act 1984 for the purposes of sub-paragraph (1) of this paragraph, the reference to the destruction of a sample under section 63R of that Act is a reference to the destruction of a sample under paragraph 43 of this Schedule.

[...].

(4) In paragraph 34 "recordable offence" has—

(a) in relation to a detainee in England or Wales, the meaning given by section 118(1) of the Police and Criminal Evidence Act 1984 [...]

Paragraph 43

(1) This paragraph applies to—

(a) fingerprints taken under paragraph 34,
(b) a DNA profile derived from a DNA sample taken under paragraph 34,
(c) relevant physical data taken or provided by virtue of paragraph 42, and
(d) a DNA profile derived from a DNA sample taken by virtue of paragraph 42.

(2) Fingerprints, relevant physical data and DNA profiles to which this paragraph applies ("paragraph 43 material") must be destroyed if it appears to the responsible chief officer of police that the taking or providing of the material or, in the case of a DNA profile, the taking of the sample from which the DNA profile was derived, was unlawful.

(3) In any other case, paragraph 43 material must be destroyed unless it is retained under a power conferred by paragraph 44, 46 or 47.

(4) Paragraph 43 material which ceases to be retained under a power mentioned in sub-paragraph (3) may continue to be retained under any other power which applies to it.

(5) Nothing in this paragraph prevents a relevant search, in relation to paragraph 43 material, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

(6) For the purposes of sub-paragraph (5), "a relevant search" is a search carried out for the purpose of checking the material against—

(a) other fingerprints or samples taken under paragraph 34 or a DNA profile derived from such a sample,

[...]

(c) fingerprints or samples taken under paragraph 10 or 12 of Schedule 8 to the Terrorism Act 2000 or a DNA profile derived from a sample taken under one of those paragraphs,

[...]

(e) material to which section 18 of the Counter-Terrorism Act 2008 applies,
(f) any of the fingerprints, data or samples obtained under paragraph 1 or 4 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011, or information derived from such samples,
(g) any of the fingerprints, samples and information mentioned in section 63A(1)(a) and (b) of the Police and Criminal Evidence Act 1984 (checking of fingerprints and samples) [...]

Paragraph 44

(1) Paragraph 43 material may be retained indefinitely in the case of a detainee who—

(a) has previously been convicted of a recordable offence (other than a single exempt conviction), [...], or
(b) is so convicted before the end of the period within which the material may be retained by virtue of this paragraph.

(2) In sub-paragraph (1)—

(a) the reference to a recordable offence includes an offence under the law of a country or territory outside the United Kingdom where the act constituting the offence would constitute—

(i) a recordable offence under the law of England and Wales if done there,[...] (and, in the application of sub-paragraph (1) where a person has previously been convicted, this applies whether or not the act constituted such an offence when the person was convicted);

[...]

(3) In the case of a person who has no previous convictions, or only one exempt conviction, the material may be retained until the end of the retention period specified in sub-paragraph (4).

(4) The retention period is—

(a) in the case of fingerprints or relevant physical data, the period of 6 months beginning with the date on which the fingerprints or relevant physical data were taken or provided, and
(b) in the case of a DNA profile, the period of 6 months beginning with the date on which the DNA sample from which the profile was derived was taken (or, if the profile was derived from more than one DNA sample, the date on which the first of those samples was taken).

Paragraph 46

(1) Paragraph 43 material may be retained for as long as a national security determination made by a chief officer of police has effect in relation to it.

(2) A national security determination is made if a chief officer of police determines that it is necessary for any paragraph 43 material to be retained for the purposes of national security.

(3) A national security determination—

(a) must be made in writing,
(b) has effect for a maximum of 5 years beginning with the date on which the determination is made, and
(c) may be renewed.

(4) In this paragraph "chief officer of police" means—

(a) a chief officer of police of a police force in England and Wales
[...]

Paragraph 48

(1) If fingerprints or relevant physical data are required by paragraph 43 to be destroyed, any copies of the fingerprints or relevant physical data held by a police force must also be destroyed.

(2) If a DNA profile is required by that paragraph to be destroyed, no copy may be retained by a police force except in a form which does not include information which identifies the person to whom the DNA profile relates.

Paragraph 49

(1) This paragraph applies to—

(a) samples taken under paragraph 34, or
(b) samples taken by virtue of paragraph 42.

(2) Samples to which this paragraph applies must be destroyed if it appears to the responsible chief officer of police that the taking of the sample was unlawful.

(3) Subject to this, the rule in sub-paragraph (4) or (as the case may be) (5) applies.

(4) A DNA sample to which this paragraph applies must be destroyed—

(a) as soon as a DNA profile has been derived from the sample, or
(b) if sooner, before the end of the period of 6 months beginning with the date on which the sample was taken.

(5) Any other sample to which this paragraph applies must be destroyed before the end of the period of 6 months beginning with the date on which it was taken.

(6) Nothing in this paragraph prevents a relevant search, in relation to samples to which this paragraph applies, from being carried out within such time as may reasonably be required for the search if the responsible chief officer of police considers the search to be desirable.

(7) In this paragraph "a relevant search" has the meaning given by paragraph 43(6).

Paragraph 50

(1) Any material to which paragraph 43 or 49 applies must not be used other than—

(a) in the interests of national security,
(b) for the purposes of a terrorist investigation, as defined by section 32 of the Terrorism Act 2000,
(c) for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution, or
(d) for purposes related to the identification of a deceased person or of the person to whom the material relates.

(2) Subject to sub-paragraph (1), a relevant search (within the meaning given by paragraph 43(6)) may be carried out in relation to material to which paragraph 43 or 49 applies if the responsible chief officer of police considers the search to be desirable.

(3) Material which is required by paragraph 43 or 49 to be destroyed must not at any time after it is required to be destroyed be used—

(a) in evidence against the person to whom the material relates, or
(b) for the purposes of the investigation of any offence.

(4) In this paragraph—

(a) the reference to using material includes a reference to allowing any check to be made against it and to disclosing it to any person;
(b) the references to an investigation and to a prosecution include references, respectively, to any investigation outside the United Kingdom of any crime or suspected crime and to a prosecution brought in respect of any crime in a country or territory outside the United Kingdom.

Paragraph 51

In paragraphs 43 to 50—

"DNA profile" means any information derived from a DNA sample;

"DNA sample" means any material that has come from a human body and consists of or includes human cells;

"fingerprints" has the meaning given by section 65(1) of the Police and Criminal Evidence Act 1984; [...]

Regulation of Investigatory Powers Act 2000

Section 49 – Notices requiring disclosure

[...]

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds–

(a) that a key to the protected information is in the possession of any person,
(b) that the imposition of a disclosure requirement in respect of the protected information is–

(i) necessary on grounds falling within subsection (3), or
(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and
(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

Investigatory Powers Act 2016

Section 199 – Bulk personal datasets: interpretation

(1) For the purposes of this Part, an intelligence service retains a bulk personal dataset if—

(a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals,
(b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions,

(c) after any initial examination of the contents, the intelligence service retains the set for the purpose of the exercise of its functions, and
(d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.

Section 200 – Requirement for authorisation by warrant: general

(1) An intelligence service may not exercise a power to retain a bulk personal dataset unless the retention of the dataset is authorised by a warrant under this Part.

(2) An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised by a warrant under this Part.

(3) For the purposes of this Part, there are two kinds of warrant—

(a) a warrant, referred to in this Part as "a class BPD warrant" , authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset of a class described in the warrant;
(b) a warrant, referred to in this Part as "a specific BPD warrant", authorising an intelligence service to retain, or to retain and examine, any bulk personal dataset described in the warrant.

Section 201 – Exceptions to section 200(1) and (2)

(1) Section 200(1) or (2) does not apply to the exercise of a power of an intelligence service to retain or (as the case may be) examine a bulk personal dataset if the intelligence service obtained the bulk personal dataset under a warrant or other authorisation issued or given under this Act.

(2) Section 200(1) or (2) does not apply at any time when a bulk personal dataset is being retained or (as the case may be) examined for the purpose of enabling any of the information contained in it to be destroyed.

Section 205 – Specific BPD warrants

(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the Secretary of State for a specific BPD warrant in the following cases.

(2) Case 1 is where—

(a) the intelligence service is seeking authorisation to retain, or to retain and examine, a bulk personal dataset, and
(b) the bulk personal dataset does not fall within a class described in a class BPD warrant.

(3) Case 2 is where—

(a) the intelligence service is seeking authorisation to retain, or to retain and examine, a bulk personal dataset, and
(b) the bulk personal dataset falls within a class described in a class BPD warrant but either—

(i) the intelligence service is prevented by section 202(1), (2) or (3) from retaining, or retaining and examining, the bulk personal dataset in reliance on the class BPD warrant, or
(ii) the intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

(4) The application must include—

(a) a description of the bulk personal dataset to which the application relates, and
(b) in a case where the intelligence service is seeking authorisation for the examination of the bulk personal dataset, the operational purposes which it is proposing should be specified in the warrant (see section 212).

(5) Where subsection (3)(b)(i) applies, the application must include an explanation of why the intelligence service is prevented by section 202(1), (2) or (3) from retaining, or retaining and examining, the bulk personal dataset in reliance on a class BPD warrant.

(6) The Secretary of State may issue the warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security,
(ii) for the purposes of preventing or detecting serious crime, or
(iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,
(c) where the warrant authorises the examination of a bulk personal dataset, the Secretary of State considers that—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of the bulk personal dataset is or may be necessary, and
(ii) the examination of the bulk personal dataset for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary,

(d) the Secretary of State considers that the arrangements made by the intelligence service for storing the bulk personal dataset and for protecting it from unauthorised disclosure are satisfactory, and
(e) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.

(7) The fact that a specific BPD warrant would authorise the retention, or the retention and examination, of bulk personal datasets relating to activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on grounds falling within subsection (6)(a).

(8) A specific BPD warrant relating to a bulk personal dataset ("dataset A") may also authorise the retention or examination of

other bulk personal datasets ("replacement datasets") that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

(9) An application for a specific BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

Section 207 – Protected data: power to impose conditions

Where the Secretary of State decides to issue a specific BPD warrant, the Secretary of State may impose conditions which must be satisfied before protected data retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.

Section 208 – Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary on grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a),
(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and
(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, whether—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset is or may be necessary, and
(ii) the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset is

necessary as mentioned in section 204(3)(c)(ii) or (as the case may be) section 205(6)(c)(ii).

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and
(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to issue a class BPD warrant or a specific BPD warrant, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a class BPD warrant or a specific BPD warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

Sections 213 – Duration of warrants

(1) A class BPD warrant or a specific BPD warrant ceases to have effect at the end of the relevant period (see subsection (2)) unless—

(a) it is renewed before the end of that period (see section 214), or
(b) it is cancelled or (in the case of a specific BPD warrant) otherwise ceases to have effect before the end of that period (see sections 209 and 218).

(2) In this section, "the relevant period" —

(a) in the case of an urgent specific BPD warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;
(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or
(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a), a specific BPD warrant is an "urgent specific BPD warrant" if—

(a) the warrant was issued without the approval of a Judicial Commissioner, and
(b) the Secretary of State considered that there was an urgent need to issue it.

(4) For provision about the renewal of warrants, see section 214.

Section 214 – Renewal of warrants

(1) If the renewal conditions are met, a class BPD warrant or a specific BPD warrant may be renewed, at any time during the renewal period, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary on grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a),
(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by the conduct,
(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that the Secretary of State considers that—

(i) each of the specified operational purposes (see section 212) is a purpose for which the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset continues to be, or may be, necessary, and
(ii) the examination of bulk personal datasets of that class or (as the case may be) the bulk personal dataset

continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) "The renewal period" means—

(a) in the case of an urgent specific BPD warrant which has not been renewed, the relevant period;
(b) in any other case, the period of 30 days ending with the day at the end of which the warrant would otherwise cease to have effect.

(4) The decision to renew a class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(5) Section 207 (protected data: power to impose conditions) applies in relation to the renewal of a specific BPD warrant as it applies in relation to the issue of such a warrant (whether or not any conditions have previously been imposed in relation to the warrant under that section).

(6) Section 208 (approval of warrants by Judicial Commissioner) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

(7) In this section—

"the relevant period" has the same meaning as in section 213;

"urgent specific BPD warrant" is to be read in accordance with subsection (3) of that section.

Section 215 – Modification of warrants

(1) The provisions of a class BPD warrant or a specific BPD warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications which may be made under this section are—

(a) in the case of a class BPD warrant, adding, varying or removing any operational purpose specified in the warrant as a purpose for which bulk personal datasets of a class described in the warrant may be examined;
(b) in the case of a specific BPD warrant, adding, varying or removing any operational purpose specified in the warrant as a purpose for which the bulk personal dataset described in the warrant may be examined.

(3) In this section—

(a) a modification adding or varying any operational purpose is referred to as a "major modification", and
(b) a modification removing any operational purpose is referred to as a "minor modification".

(4) A major modification—

(a) must be made by the Secretary of State, and
(b) may be made only if the Secretary of State considers that it is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (see section 204(3)(a) or (as the case may be) section 205(6)(a)).

(5) Except where the Secretary of State considers that there is an urgent need to make the modification, a major modification has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(6) A minor modification may be made by—

(a) the Secretary of State, or
(b) a senior official acting on behalf of the Secretary of State.

(7) Where a minor modification is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(8) If at any time a person mentioned in subsection (6) considers that any operational purpose specified in a warrant is no longer a purpose for which the examination of any bulk personal datasets to which the warrant relates is or may be necessary, the person must modify the warrant by removing that operational purpose.

(9) The decision to modify the provisions of a class BPD warrant or a specific BPD warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person. This is subject to subsection (10).

(10) If it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument may be signed by a senior official designated by the Secretary of State for that purpose.

(11) In such a case, the instrument making the modification must contain a statement that—

(a) it is not reasonably practicable for the instrument to be signed by the Secretary of State, and
(b) the Secretary of State has personally and expressly authorised the making of the modification.

Section 216 – Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on

an application for judicial review, and
(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 215, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 215, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification.

Section 217 – Approval of major modifications made in urgent cases

(1) This section applies where—

(a) the Secretary of State makes a major modification of a class BPD warrant or a specific BPD warrant without the approval of a Judicial Commissioner, and
(b) the Secretary of State considered that there was an urgent need to make the modification.

(2) The Secretary of State must in form a Judicial Commissioner that the modification has been made.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to make the modification, and
(b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the third working day after the day on which the modification was made.

(4) If the Judicial Commissioner refuses to approve the decision to make the modification—

(a) the warrant (unless it no longer has effect) has effect as if the modification had not been made, and
(b) the person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant by virtue of that modification stops as soon as possible, and section 216(4) does not apply in relation to the refusal to approve the decision.

(5) Nothing in this section affects the lawfulness of—

(a) anything done in reliance on the warrant by virtue of the modification before the modification ceases to have effect;
(b) if anything is in the process of being done in reliance on the warrant by virtue of the modification when the modification ceases to have effect—

(i) anything done before that thing could be stopped, or
(ii) anything done which it is not reasonably practicable to stop.

Section 218 – Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a class BPD warrant or a specific BPD warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers that any of the cancellation conditions are met in relation to a class BPD warrant or a specific BPD warrant, the person must cancel the warrant.

(3) The cancellation conditions are—

(a) that the warrant is no longer necessary on any grounds falling within section 204(3)(a) or (as the case may be) section 205(6)(a);
(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct;

(c) where the warrant authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that the examination of bulk personal datasets of that class or (as the case may be) of the bulk personal dataset is no longer necessary for any of the specified operational purposes (see section 212).

Section 221 – Safeguards relating to examination of bulk personal datasets

(1) The Secretary of State must ensure, in relation to every class BPD warrant or specific BPD warrant which authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that arrangements are in force for securing that—

(a) any selection of data contained in the datasets (or dataset) for examination is carried out only for the specified purposes (see subsection (2)), and
(b) the selection of any such data for examination is necessary and proportionate in all the circumstances.

(2) The selection of data contained in bulk personal datasets for examination is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 212.

(3) The Secretary of State must also ensure, in relation to every specific BPD warrant which specifies conditions imposed under section 207, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant.

(4) In this section "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

Section 224 – Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any data contained in a bulk personal dataset retained in reliance on a class BPD warrant or a specific BPD warrant,
(b) the person knows or believes that the selection of that data is in breach of a requirement specified in subsection (2), and
(c) the person deliberately selects that data in breach of that requirement.

(2) The requirements specified in this subsection are that any selection for examination of the data—

(a) is carried out only for the specified purposes (see subsection (3)),
(b) is necessary and proportionate, and
(c) if the data is protected data, satisfies any conditions imposed under section 207.

(3) The selection for examination of the data is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 212. In this subsection, "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of [paragraph 24(2) of Schedule 22 to the Sentencing Act 2020]1), or
(ii) to a fine, or to both;

[...]

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(5) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions; [...]

Protection of Freedoms Act 2012

Section 20 – Appointment and functions of Commissioner

(1) The Secretary of State must appoint a Commissioner to be known as the Commissioner for the Retention and Use of Biometric Material (referred to in this section and section 21 as "the Commissioner").

(2) It is the function of the Commissioner to keep under review—

(a) every national security determination made or renewed under—

(i) section 63M of the Police and Criminal Evidence Act 1984 (section 63D material retained for purposes of national security),
(ii) paragraph 20E of Schedule 8 to the Terrorism Act 2000 (paragraph 20A material retained for purposes of national security),
(iii) section 18B of the Counter-Terrorism Act 2008 (section 18 material retained for purposes of national security),
(iv) paragraph 11 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011 (paragraph 6 material retained for purposes of national security),
(iva) paragraph 46 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019, [...]

(b) the uses to which material retained pursuant to a national security determination is being put.

(3) It is the duty of every person who makes or renews a national security determination under a provision mentioned in subsection (2)(a) to—

(a) send to the Commissioner a copy of the determination or renewed determination, and the reasons for making or renewing the determination, within 28 days of making or renewing it, and
(b) disclose or provide to the Commissioner such documents and information as the Commissioner may require for the purpose of carrying out the Commissioner's functions under subsection (2).

(4) If, on reviewing a national security determination made or renewed under a provision mentioned in subsection (2)(a), the Commissioner concludes that it is not necessary for any material retained pursuant to the determination to be so retained, the Commissioner may order the destruction of the material if the condition in subsection (5) is met.

(5) The condition is that the material retained pursuant to the national security determination is not otherwise capable of being lawfully retained.

(6) The Commissioner also has the function of keeping under review—

(a) the retention and use in accordance with sections 63A and 63D to 63T of the Police and Criminal Evidence Act 1984 of—

(i) any material to which section 63D or 63R of that Act applies (fingerprints, DNA profiles and samples), and
(ii) any copies of any material to which section 63D of that Act applies (fingerprints and DNA profiles),

(b) the retention and use in accordance with paragraphs 20A to 20J of Schedule 8 to the Terrorism Act 2000 of—

(i) any material to which paragraph 20A or 20G of that Schedule applies (fingerprints, relevant physical data, DNA profiles and samples), and
(ii) any copies of any material to which paragraph 20A of that Schedule applies (fingerprints, relevant physical data and DNA profiles),

(c) the retention and use in accordance with sections 18 to 18E of the Counter-Terrorism Act 2008 of—

(i) any material to which section 18 of that Act applies (fingerprints, DNA samples and DNA profiles), and
(ii) any copies of fingerprints or DNA profiles to which section 18 of that Act applies,

(d) the retention and use in accordance with paragraphs 5 to 14 of Schedule 6 to the Terrorism Prevention and Investigation Measures Act 2011 of—

(i) any material to which paragraph 6 or 12 of that Schedule applies (fingerprints, relevant physical data, DNA profiles and samples), and
(ii) any copies of any material to which paragraph 6 of that Schedule applies (fingerprints, relevant physical data and DNA profiles),

(e) the retention and use in accordance with paragraphs 43 to 51 of Schedule 3 to the Counter-Terrorism and Border Security Act 2019 of—

(i) any material to which paragraph 43 or 49 of that Schedule applies (fingerprints, relevant physical data, DNA profiles and samples), and
(ii) any copies of any material to which paragraph 43 of that Schedule applies (fingerprints, relevant physical data and DNA profiles).

(7) But subsection (6) does not apply so far as the retention or use of the material falls to be reviewed by virtue of subsection (2).

[...]

(9) The Commissioner also has functions under sections 63F(5)(c) and 63G (giving of consent in relation to the retention of certain section 63D material).

(10) The Commissioner is to hold office in accordance with the terms of the Commissioner's appointment; and the Secretary of State may pay in respect of the Commissioner any expenses, remuneration or

allowances that the Secretary of State may determine.

(11) The Secretary of State may, after consultation with the Commissioner, provide the Commissioner with—

(a) such staff, and
(b) such accommodation, equipment and other facilities, as the Secretary of State considers necessary for the carrying out of the Commissioner's functions.

Section 21 – Reports by Commissioner

(1) The Commissioner must make a report to the Secretary of State about the carrying out of the Commissioner's functions as soon as reasonably practicable after the end of—

(a) the period of 9 months beginning when this section comes into force, and
(b) every subsequent 12 month period.

(2) The Commissioner may also, at any time, make such report to the Secretary of State on any matter relating to the Commissioner's functions as the Commissioner considers appropriate.

(3) The Secretary of State may at any time require the Commissioner to report on any matter relating to the Commissioner's functions.

(4) On receiving a report from the Commissioner under this section, the Secretary of State must—

(a) publish the report, and
(b) lay a copy of the published report before Parliament.

(5) The Secretary of State may, after consultation with the Commissioner, exclude from publication any part of a report under this section if, in the opinion of the Secretary of State, the publication of that part would be contrary to the public interest or prejudicial to national security.

Section 26 – Requirement to notify and obtain consent before processing biometric information

(1) This section applies in relation to any processing of a child's biometric information by or on behalf of the relevant authority of—

(a) a school,
(b) a 16 to 19 Academy, or
(c) a further education institution.

(2) Before the first processing of a child's biometric information on or after the coming into force of subsection (3), the relevant authority must notify each parent of the child—

(a) of its intention to process the child's biometric information, and
(b) that the parent may object at any time to the processing of the information.

(3) The relevant authority must ensure that a child's biometric information is not processed unless—

(a) at least one parent of the child consents to the information being processed, and
(b) no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed.

(4) Section 27 makes further provision about the requirement to notify parents and the obtaining and withdrawal of consent (including when notification and consent are not required).

(5) But if, at any time, the child—

(a) refuses to participate in, or continue to participate in, anything that involves the processing of the child's biometric information, or
(b) otherwise objects to the processing of that information,
the relevant authority must ensure that the information is not processed, irrespective of any consent given by a parent of the child under subsection (3).

(6) Subsection (7) applies in relation to any child whose biometric information, by virtue of this section, may not be processed.

(7) The relevant authority must ensure that reasonable alternative means are available by which the child may do, or be subject to, anything which the child would have been able to do, or be subject to, had the child's biometric information been processed.

Section 29 – Code of practice for surveillance camera systems

(1) The Secretary of State must prepare a code of practice containing guidance about surveillance camera systems.

(2) Such a code must contain guidance about one or more of the following—

(a) the development or use of surveillance camera systems,
(b) the use or processing of images or other information obtained by virtue of such systems.

(3) Such a code may, in particular, include provision about—

(a) considerations as to whether to use surveillance camera systems,
(b) types of systems or apparatus,
(c) technical standards for systems or apparatus,
(d) locations for systems or apparatus,
(e) the publication of information about systems or apparatus,
(f) standards applicable to persons using or maintaining systems or apparatus,
(g) standards applicable to persons using or processing information obtained by virtue of systems,
(h) access to, or disclosure of, information so obtained,
(i) procedures for complaints or consultation.

(4) Such a code—

(a) need not contain provision about every type of surveillance camera system,
(b) may make different provision for different purposes.

(5) In the course of preparing such a code, the Secretary of State must consult—

(a) such persons appearing to the Secretary of State to be representative of the views of persons who are, or are likely to be, subject to the duty under section 33(1) (duty to have regard to the code) as the Secretary of State considers appropriate,
(b) the National Police Chiefs' Council,
(c) the Information Commissioner,
(d) the Investigatory Powers Commissioner,
(e) the Surveillance Camera Commissioner,
(f) the Welsh Ministers, and
(g) such other persons as the Secretary of State considers appropriate.

(6) In this Chapter "surveillance camera systems" means—

(a) closed circuit television or automatic number plate recognition systems,
(b) any other systems for recording or viewing visual images for surveillance purposes,
(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or
(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

(7) In this section—

"processing" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(4) and (14) of that Act).

Section 33 – Effect of code

(1) A relevant authority must have regard to the surveillance camera code when exercising any functions to which the code relates.

[...]

(5) In this section "relevant authority" means—

(a) a local authority within the meaning of the Local Government Act 1972,
(b) the Greater London Authority,
(c) the Common Council of the City of London in its capacity as a local authority,
(d) the Sub-Treasurer of the Inner Temple or the Under-Treasurer of the Middle Temple, in their capacity as a local authority,
(e) the Council of the Isles of Scilly,
(f) a parish meeting constituted under section 13 of the Local Government Act 1972,
(g) a police and crime commissioner,
(h) the Mayor's Office for Policing and Crime,
(i) the Common Council of the City of London in its capacity as a police authority,
(j) any chief officer of a police force in England and Wales,
(k) any person specified or described by the Secretary of State in an order made by statutory instrument.

Section 34 – Commissioner in relation to code

(1) The Secretary of State must appoint a person as the Surveillance Camera Commissioner (in this Chapter "the Commissioner").

(2) The Commissioner is to have the following functions—

(a) encouraging compliance with the surveillance camera code,
(b) reviewing the operation of the code, and
(c) providing advice about the code (including changes to it or breaches of it).

(3) The Commissioner is to hold office in accordance with the terms of the Commissioner's appointment; and the Secretary of State may pay in respect of the Commissioner any expenses, remuneration or allowances that the Secretary of State may determine.

(4) The Secretary of State may, after consultation with the Commissioner, provide the Commissioner with—

(a) such staff, and
(b) such accommodation, equipment and other facilities, as the

Secretary of State considers necessary for the carrying out of the Commissioner's functions.

Equality Act 2010

Section 4 – The protected characteristics

The following characteristics are protected characteristics—

age;
disability;
gender reassignment;
marriage and civil partnership;
pregnancy and maternity;
race;
religion or belief;
sex;
sexual orientation.

Section 13 – Direct discrimination

(1) A person (A) discriminates against another (B) if, because of a protected characteristic, A treats B less favourably than A treats or would treat others.

(2) If the protected characteristic is age, A does not discriminate against B if A can show A's treatment of B to be a proportionate means of achieving a legitimate aim.

(3) If the protected characteristic is disability, and B is not a disabled person, A does not discriminate against B only because A treats or would treat disabled persons more favourably than A treats B.

(4) If the protected characteristic is marriage and civil partnership, this section applies to a contravention of Part 5 (work) only if the treatment is because it is B who is married or a civil partner.

(5) If the protected characteristic is race, less favourable treatment includes segregating B from others.

(6) If the protected characteristic is sex—

(a) less favourable treatment of a woman includes less favourable treatment of her because she is breast-feeding;
(b) in a case where B is a man, no account is to be taken of special treatment afforded to a woman in connection with pregnancy or childbirth.

(7) Subsection (6)(a) does not apply for the purposes of Part 5 (work).

(8) This section is subject to sections 17(6) and 18(7).

Section 19 – Indirect discrimination

(1) A person (A) discriminates against another (B) if A applies to B a provision, criterion or practice which is discriminatory in relation to a relevant protected characteristic of B's.

(2) For the purposes of subsection (1), a provision, criterion or practice is discriminatory in relation to a relevant protected characteristic of B's if—

(a) A applies, or would apply, it to persons with whom B does not share the characteristic,
(b) it puts, or would put, persons with whom B shares the characteristic at a particular disadvantage when compared with persons with whom B does not share it,
(c) it puts, or would put, B at that disadvantage, and
(d) A cannot show it to be a proportionate means of achieving a legitimate aim.

Section 149 – Public sector equality duty

(1) A public authority must, in the exercise of its functions, have due regard to the need to—

(a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;
(b) advance equality of opportunity between persons who share

a relevant protected characteristic and persons who do not share it;
(c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

(2) A person who is not a public authority but who exercises public functions must, in the exercise of those functions, have due regard to the matters mentioned in subsection (1).

(3) Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to—

(a) remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic;
(b) take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it;
(c) encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.

(4) The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

(5) Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to—

(a) tackle prejudice, and
(b) promote understanding.

(6) Compliance with the duties in this section may involve treating some persons more favourably than others; but that is not to be taken as permitting conduct that would otherwise be prohibited by or under this Act.

Draft EU Proposal for a Regulation laying down harmonised rules on artificial intelligence (COM/2021/206 final)

Article 3 – Definitions

[...]

(36) 'remote biometric identification system' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified;

[...]

(40) 'law enforcement authority' means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

Article 5

(1) The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group

of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;
(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific potential victims of crime, including missing children;
(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

[...]

(3) As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric

identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use. The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

(4) A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

Article 10 – Data and data governance

[...]

(3) Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

Article 14 – Human oversight

(1) High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

(2) Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.

(3) Human oversight shall be ensured through either one or all of the following measures:

(a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;
(b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

(4) The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

(a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;
(b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;
(c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;
(d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse

the output of the high-risk AI system;
(e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

(5) For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

Article 17 – Quality management system

(1) Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;
(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;
(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;
(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;
(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into

service of high-risk AI systems;
(g) the risk management system referred to in Article 9;
(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61;
(i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62;
(j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;
(k) systems and procedures for record keeping of all relevant documentation and information;
(l) resource management, including security of supply related measures;
(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

(2) The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.

Article 19 – Conformity assessment

(1) Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.

Article 29 – Obligations of users of high-risk AI systems

[...]

(4) Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in

the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.

Article 43 – Conformity assessment

(1) For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

(a) the conformity assessment procedure based on internal control referred to in Annex VI;
(b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII. For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

(2) For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide

for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to 101 of that Directive.

(3) For high-risk AI systems, to which legal acts listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter 2 of this Title shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply. For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts. Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chapter 2 of this Title.

(4) High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user. For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

(5) The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII in order to introduce elements of the conformity assessment procedures that become necessary in light of technical

progress.

(6) The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

Article 52 – Transparency obligations for certain AI systems

[...]

(2) Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

Article 64 – Access to data and documentation

[...]

(2) Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

Article 69 – Codes of conduct

[...]

(1) The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems

of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.

Annex III – High-risk AI systems referred to in Article 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

(1) Biometric identification and categorisation of natural persons:

(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;

[...]

The quoted legislation has been reproduced as at June 2021.

Annex 2: The Review team

Matthew Ryder QC	Senior Barrister, Matrix Chambers
Jessica Jones	Barrister, Matrix Chambers
Javier Ruiz	Independent Consultant on data ethics
Samuel Rowe	Pupil Barrister, 5 Essex Court

Annex 3: Advisory Board

Lillian Edwards	Professor of Law, Innovation and Society, Newcastle Law School
Anneke Lucasson	Professor of Clinical Genetics within Medicine, University of Southampton
Marion Oswald	Professor, School of Law, Northumbria University
Matthew Rice	Scotland Director, Open Rights Group
Renate Samson	Senior Policy Advisor, Open Data Institute
Pamela Ugwudike	Associate Professor of Criminology, University of Southampton
Edgar Whitley	Associate Professor of Information Management, London School of Economics

All organisational affiliations correct at time of publication.

Annex 4: Consultees

Amba Kak, AI Now, 8 October 2020
Megan Gould, Liberty, 8 October 2020
Elaine Hamilton and **David Scott**, Scottish Biometrics Commissioner Bill, 13 October 2020
Michael Gribben, **Ben Dellot** and **Jessica Smith**, Centre for Data Ethics and Innovation, 16 October 2020
Ali Shah, **Anne Russell**, **Ali Hall**, Information Commissioner's Office, 19 October 2020
Baroness Susan Williams, **Kit Malthouse MP**, 20 October 2020
Professor Paul Wiles, Biometrics Commissioner, 9 November 2020
Professor Gillian Tully CBE, Forensic Science Regulator, 11 November 2020
Dr Daragh Murray, University of Essex, 12 November 2020
Tony Porter, Surveillance Camera Commissioner, 9 December 2020
Detective Chief Superintendent Chris Todd, West Midlands Police, 7 January 2021
Rachel Tuffin OBE, College of Policing, 19 January 2021
Silkie Carlo, Big Brother Watch, 20 January 2021
Dr Suzanne Shale, London Policing Ethics Panel, 25 January 2021
Assistant Chief Constable Dr Iain Raphael and **David Hudson**, College of Policing, 1 February 2021
Lindsey Chiswick, Metropolitan Police, 2 February 2021
Robin Allen QC and **Dee Masters**, Cloisters Chambers, 9 February 2021

All organisational affiliations correct at time of interview.

About the author

Matthew Ryder QC is a recognised legal expert in the fields of human rights; equality and diversity; crime, policing and surveillance; and data, technology and information. Between 2016 and 2018 he was Deputy Mayor for London on social integration, social mobility and community engagement, and was also a member of the Lammy Review of racial bias and BAME representation in the criminal justice system.

About the Ada Lovelace Institute

The Ada Lovelace Institute was established by the Nuffield Foundation in early 2018, in collaboration with the Alan Turing Institute, the Royal Society, the British Academy, the Royal Statistical Society, the Wellcome Trust, Luminate, techUK and the Nuffield Council on Bioethics.

The mission of the Ada Lovelace Institute is to ensure that data and AI work for people and society. We believe that a world where data and AI work for people and society is a world in which the opportunities, benefits and privileges generated by data and AI are justly and equitably distributed and experienced.

We recognise the power asymmetries that exist in ethical and legal debates around the development of data-driven technologies, and will represent people in those conversations. We focus not on the types of technologies we want to build, but on the types of societies we want to build.

Through research, policy and practice, we aim to ensure that the transformative power of data and AI is used and harnessed in ways that maximise social wellbeing and put technology at the service of humanity.

We are funded by the Nuffield Foundation, an independent charitable trust with a mission to advance social well-being. The Foundation funds research that informs social policy, primarily in education, welfare and justice. It also provides opportunities for young people to develop skills and confidence in STEM and research. In addition to the Ada Lovelace Institute, the Foundation is also the founder and co-funder of the Nuffield Council on Bioethics and the Nuffield Family Justice Observatory.

Find out more:

Website: adalovelaceinstitute.org
Twitter: @AdaLovelaceInst
Email: hello@adalovelaceinstitute.org

Preferred citation: Ryder QC, M. (2022). *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales.* Ada Lovelace Institute. Available at: https://www.adalovelaceinstitute.org/report/ryder-review-biometrics

ISBN: 978-1-7397950-1-6