The Frank Dawtry Memorial Lecture delivered at the University of Leeds: Tuesday 11 February, 2020

INTRODUCTION

Thank you for doing me the honour of inviting me to give the Frank Dawtry Memorial lecture.

I am aware that the audience for this lecture might have different backgrounds so I will keep my remarks of a kind that I hope will be clear to everyone. We can, of course, discuss detailed issues later as questions.

MY ROLE AS COMMISSIONER

Presently, as you know I am the UK's Biometrics Commissioner, or to be more precise 'the Commissioner for the Retention and Use of Biometric Material'. In fact my remit only covers the police use of biometrics for criminal investigation and prosecution and for purposes of national security. My role was created by the Protection of Freedoms Act (hereafter 'PoFA') in 2012 and is limited to the police use of DNA and fingerprints.

In the UK responsibility for policing and crime investigation is devolved in the case of Scotland and Northern Ireland and so my remit only covers England and Wales. National security, however, is not devolved and my remit covers the UK. I am required to produce an annual report for the Home Secretary and she is in turn required to lay that report before Parliament, in other words it is published. Beyond that I have two quasi-judicial functions in relation to police retention of DNA and fingerprints. I am often referred to as a 'regulator' but I am not and have no regulatory powers. Instead the most important aspect of my role is to provide independent oversight that Parliament thought necessary in giving the police considerable powers to use biometrics.

Strictly speaking my role is quite limited but I, like the first Commissioner, have felt it right that I should report to the Home Secretary on the growth of new biometrics and policing interest in them. Given that biometrics are classified as 'sensitive' data in legislation[1] then one can see why independent oversight might be thought useful to maintain public trust. Governments tend to create Commissioners when they feel the need to bolster support for a measure but can soon come to regret having limited Ministerial authority. My helpful comments therefore have not always been welcomed but that probably inevitably goes with being an Independent Commissioner. Certainly, there is no way in which I can stop the media, home and foreign, or the police asking me to comment on use of the new biometrics.

[1] In the Data Protection Act 2018.

WHAT ARE BIOMETRICS?

But I am getting ahead of what I want to talk about so let me go back to the basics. What are 'biometrics'? Biometrics are any aspect of our biology that can practically be used to try and uniquely identify us against the mass of our fellow humans. As far as police use of biometrics is concerned the interest extends beyond authenticating identity to the forensic possibility of such biometrics leaving traces at a crime scene or on a victim.

HISTORY OF BIOMETRIC USE BY THE POLICE IN ENGLAND & WALES

The use of biometrics by the police in the UK is almost as old as modern policing itself, having its origin in the late nineteenth century and involved the police taking fingerprints and photographs. All of you will have seen examples of old police mug shots and how they were used to search for wanted people. However, this early use of biometrics was limited since searching for matches involved making comparisons with paper-based reference collections, which was slow, constrained by the need to keep reference collections manageable in size and therefore limited usually to local collections. These early biometrics were useful for policing but were limited in scope. The limitations were acceptable since police forces were also local and offenders assumed to come from a local criminal class.

A hundred years later, the growth of computing and the realisation that DNA could be used for forensic purposes led to a technical revolution. DNA profiles can be derived from DNA samples and since they are expressed digitally can be stored on a computer database. This removed many of the previous limitations on the police use of biometrics because machine digital matching became possible and the reference collection being searched could be national, or even international. DNA was the first true modern police 'biometric' and a national DNA database was set up in 1995 by the Home Office, the first of its kind anywhere. Fingerprints later followed and local paper collections were replaced by a national fingerprint database. Digitally matching photographs proved more difficult and had to wait for the next generation of technical changes.

A further technical revolution is happening now and is driven by our ability to build ever larger databases and then to use artificial intelligence (AI) on those databases to develop algorithms for biometric matching. This development of AI-driven analytics has speeded up the development of a wide range of new technologies and will affect all areas of our future life. As far as the police use of biometrics is concerned the first visible result is the new ability to use digital facial images in a similar way to DNA and fingerprints: in other words those old mug shots have become modern digital biometrics. The growth of the new AI-driven technologies has been very rapid and has meant that over the last five years facial matching algorithms have improved exponentially. However, facial matching is just the first of a range of new biometrics that are becoming available and could be used by the police.

GOVERNANCE OF BIOMETRIC USE BY THE POLICE

The historical development of biometric use by the police in England and Wales slowly came under legislative control. The first significant governance was introduced by the Police & Criminal Evidence Act 1984 (PACE), which required police to destroy fingerprints and DNA samples that were taken during a criminal investigation if an individual was not convicted of an offence. From 2001 the police were allowed to keep biometrics indefinitely if an individual was charged but not convicted of an offence and from 2003[2] to do so even if an arrested individual was neither charged nor convicted. However, in 2008 the European Court of Human Rights held in response to a challenge to this position that England and Wales and Northern Ireland were the only Council of Europe members who allowed such indiscriminate retention of DNA and fingerprints and because this failed to strike a fair balance between public and private interests it was not proportionate.[3] In response, the Labour government passed the Crime and Security Act 2010 which reduced some retention periods but before the Act was implemented a general election intervened.

The incoming coalition government repealed that Act and instead introduced the Protection of Freedoms Act in 2012 which generally restricted the indefinite retention of DNA and fingerprints to those convicted but allows some retention for those charged but not convicted and limited retention for those arrested for more serious offences but not charged on application to the Biometrics Commissioner. The Act also allows for the retention of biometrics on grounds of national security by the granting of a National Security Determination by a Chief Officer of Police. I oversee those Determinations and can order the destruction of the biometrics if I think the Determination inappropriate. Finally, PoFA allows the police to keep the DNA profile but not the DNA sample to guard against the DNA material been used for any other purpose than that authorised.

The present situation, therefore, is that we have legislation governing the police use of biometrics which was passed in response to a judgment of the European Court of Human Rights. However, we are awaiting a further judgment from the same Court in the case of Gaughran that is expected imminently.[4] I do not want to predict what that judgment will find but on the basis of the Court's recent jurisprudence it is possible that it may require further governance changes. More directly, PoFA only governs the police use of DNA and fingerprints but not facial images or any other new biometric. Furthermore, as just explained, the usefulness of the new biometrics is been driven by the use of AI analytics, that are also being used to explore how far they could

[2]Criminal Justice and Police Act 2001 and Criminal Justice Act 2003
[3]S and Marper v United Kingdom [**2008**] **ECHR** 1581
[4] Since this lecture was given the judgement has been delivered: https://hudoc.echr.coe.int/eng#{"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-200817"]}

have other uses for policing. The Home Office has funded a trial with West Midlands Police to examine whether such analytics could be used to predict future offending. Biometrics then are just one data source that can be explored for possible police use.

OPPOSITION TO THE POLICE USE OF NEW BIOMETRICS

These developments, however, have led to some opposition. What especially galvanised public concern about the use of these new technologies were the trials carried out by the South Wales and Metropolitan Police of the use of live facial recognition (LFR) in public places. This was almost bound to raise concerns because unlike the existing police biometrics whose acquisition is complicated, digital facial image capture is easy and the subject may not even be aware that it has happened. For the same reason faces in public places can be easily scanned and matched. The use of LFR also extends the range of police surveillance of the public by new technical means. In other words, LFR is much more intrusive of individual privacy than existing biometric use. That is not to say that there may not be a public interest case that justifies in some cases such intrusion when balanced against the public benefits derived. However, the trials inevitably raised the question of whether the police use of LFR in public places is so justified?

The reaction to the police LFR trials was predictable. There were both media and political requests for greater transparency, civil rights groups questioned whether uses of LFR in public places by the police could be justified as in the public interest and a similar debate in the US led to some cities banning the use of facial matching by their police forces. In this country *Big Brother Watch* published an open letter demanding a halt in the police use of LFR which was signed by the (then) leader of an opposition party, shadow Home Secretary and Chair of the Commons Science & Technology Committee.

A legal challenge was made by *Liberty*, against South Wales Police, and *Big Brother Watch*, currently has a stayed challenge against the Metropolitan Police.

LEGAL CHALLENGES

In the South Wales Police case the Court decided that their use of LFR was consistent with the requirements of the Human Rights Act and data protection legislation and lawful in pursuit of the Police's common law power to prevent crime and arrest offenders. It also found that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of the LFR as it was used in trials by South Wales Police.[5]

The judgment considered solely the use of LFR by the police and not by any other public or indeed private body. It should also be noted that this is a judgment in the first instance and that the claimant now intends to appeal. This is not surprising given the fundamental rights at stake and

[5] R (Bridges) v CCSWP and SSHD,[2019] EWHC 2341 (Admin)

that, as is stated in the judgment, this is the first time that any court in the world has considered LFR.

It is not for me, as Commissioner, to comment on the High Court's judgment or the likely outcome of an appeal. For the present the police have a lawful basis for using LFR but should be aware that the Court stressed that its judgment related to the specific way in which South Wales Police had conducted their trial.

LEGISLATION GOVERNING THE USE OF BIOMETRICS IN ENGLAND & WALES

In addition to the common law power relied on by the High Court judgment, important legislation governing the police use of biometrics is the Data Protection Act 2018.

The Data Protection Act brought into UK law the requirements of EU regulation of the use of personal data as set out in principle in the General Data Protection Regulation (GDPR) but includes special provisions for the processing of data by law enforcement.[6] The Act is enforced by the Information Commissioner and she has already examined the use of LFR by the police,[7] has commented on the South Wales Police judgment,[8] and is investigating the use of LFR by private bodies.[9] Unlike me the Information Commissioner is a regulator and has significant powers to ensure that any use of LFR abides by the requirements of data protection legislation and she has made clear that she is prepared to use those powers if it does not.

This raises the question of whether data protection legislation covers all the matters of principle that are thought necessary to govern the police use of biometrics?.

Data protection legislation, as already explained is based on the GDPR principles that are essentially designed to protect people's privacy since privacy is a good in itself.[10] However, that value can easily conflict with other values, such as actions which deliver benefits to a collective or public interest. Tensions between different values are inevitable since very few actions simply relate to only one such value. It is in the essence of social behaviour and especially the political consideration of social behaviour that such tensions have to be decided upon and then managed. That is why a central part of previous legislation governing the police use of biometrics is how that tension should be resolved: what is the balance between the individual's right to privacy and the public benefits that will derive from police use of DNA and fingerprints? It is what lawyers refer to as 'proportionality' and it has been central to the legal challenges that have been made to the governance of the police use of DNA, fingerprints and custody images.

---

[6] See: https://ico.org.uk/for-organisations/guide-to-data-protection/
[7] https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
[8] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
[9] See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/
[10] At least that is so in the western thought tradition but not necessarily so in other traditions which place more emphasis on collectivism.

If the question of proportionality is central to the governance of the police use of biometrics then it leaves the question of how that should be decided? That in turn has two aspects: namely who should decide and on what basis?

At present we have a mixed picture on who should decide on proportionality for the police use of biometrics. For DNA and fingerprints that has been decided by Parliament and passed into statute.

In the case of the new biometrics the decision is currently being made by the police. Some police leaders are unhappy with that position since they fear that taking the decision may not be seen as legitimate and therefore risk public trust in policing. The result is that many police forces are very cautious about using the new biometrics, especially LFR. This is understandable at a time when there has been a reported decline in trust in public institutions that has also been linked to a decline in confidence in democratic government.[11]

In the South Wales Police case the court approached the question of proportionality in procedural terms by examining whether the police had procedures in place that meant that the way in which they managed their trial met tests of legality and decided that it did.

Any police use of biometrics must be compliant with data protection legislation. That means that the Information Commissioner has a role in deciding some elements of the proportionality of police use of biometrics.[12]

As things stand the Information Commissioner or the court judgments may limit some possible uses by the police of LFR. But the South Wales judgment has already revealed some tension between these two routes.[13] We are likely to see further legal challenges to biometric use by the police and such challenges will be helpful in clarifying how the police may act but will mean that the police use of new biometrics will be slowed and rely on judge-made law, something that most of the judiciary do not like doing, preferring that if there needs to be a legal response to social and technological change that it should be through legislation made by Parliament.[14]

In the past ultimately it has been for Parliament to decide what police use of biometrics is proportionate. That is because in a democracy balancing citizen's individual rights against whether any state interference in those rights is justified is a political matter to be decided by

---

[11] https://www.cambridge.org/core/journals/american-political-science-review/article/in-the-mood-for-democracy-democratic-support-as-thermostatic-opinion/D92BFDDD1565D610C38A0AA88DDBA102

[12] Such sensitive data requires that it also has a legal basis in statute, common law or royal prerogative and that it is being carried out *for substantial pubic interest and that different categories of subject's whose data is being used should be distinguished.*Such sensitive data requires that it also has a legal basis in statute, common law or royal prerogative and that it is being carried out *for substantial pubic interest and that different categories of subject's whose data is being used should be distinguished.* See the ICO's *Guide to Law Enforcement Processing.*

[13] See:https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

[14] For an eloquent statement of this position see: Sumption, J: Trials of State: Law and the Decline of Politics, London, Profile Books, 2019.

the body that has a legitimate power to make such decisions, namely Parliament. In the end it is for Parliament to decide whether we wish the police in England and Wales to use LFR or other new biometrics and if so for what purposes. The question now is whether there should be new legislation that provides specific rules for the police (and perhaps others) use of new biometrics, including LFR but also voice recognition, gait analysis, iris analysis or any other new biometric technologies as they emerge.

POSITION OF THE NEW GOVERNMENT

The May government felt that legislation to govern the use of new biometrics by the police was unnecessary and welcomed the South Wales judgment as justifying that position.

However, the Conservative Party in its recent manifesto proposed legislating and it is worth quoting that commitment in full:

> **"We will embrace new technologies and crack down on online crimes. We will create a new national cyber crime force and empower the police to safely use new technologies like biometrics and artificial intelligence, along with the use of DNA, within a strict legal framework. We will also create a world-class National Crime Laboratory."**

Manifestos are brief statements of intent and we will have to wait to see what this means in legislative terms. This intention did not feature in the Queen's speech so I assume that this will not happen in this session of Parliament.

THE POLICE RESPONSE

I have already pointed out that many police leaders are cautious about deploying the new biometrics without a clear governance framework to guide their decisions. However, two forces have been less constrained. The South Wales Police on the basis of the Cardiff High Court judgment are continuing to trial LFR in public places, most recently at a local football derby. The Metropolitan Police Service have now announced that they will proceed with operational deployment of LFR. This is a step change from trial to operational deployment. Before starting such deployment, the MPS have placed on their website a legal mandate for their use of LFR and a guidance document for the governance of the deployment. These are designed to demonstrate the legality of the use of LFR and that they are staying within the jurisprudence of the South Wales judgment. Judging that claim will have to wait because it involves an examination of the documents but also how far they do in fact govern the operational use of LFR in practice. Any significant doubt in this regard could lead to further legal challenge.

However, this is a legalistic response and what will also matter is how far the public decide that what the MPS are doing is acceptable. Our present understanding of the public(s) attitudes

comes from simple binary survey questions, without respondents knowing the details of what is being proposed and using non-random probability samples. I therefore welcome that the Ada Lovelace Institute is about to conduct methodologically more sophisticated work to try and understand how the public(s) might respond to the use of LFR by the police.[15]

The Metropolitan Police Commissioner has said that she believes that the deployment of new technology by the police is essential if the police are going to be able to respond to the policing challenges of the future, many of which spring from those same technologies. In this regard she has been talking not just about facial matching but also things like the growth of digital crime evidence. At the same time she has also said that public trust must be retained as new technologies are deployed. Like the judges, she would probably prefer that government should provided rules governing the police use of new technologies rather than leaving it to the police service. The problem is that technology is developing very fast and creating both new crime challenges and possible new technical responses but policy and legislation is moving much slower.

What the Met Commissioner's concerns do illustrate is that future biometric use by the police cannot be separated from their use of other AI-driven analytics that are using non-biometric data. Indeed the borderline between biometric and other data is becoming blurred. Compare the definition of 'biometric' I gave you earlier with that in the GDPR:

> **"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".**

The inclusion in that definition of 'behavioural characteristics' means that a much broader range of data sets used for AI-analytics will be covered by this definition of biometrics.

BIOMETRIC USE BEYOND POLICING

We are all aware that the new biometrics, such as facial matching, are being used more widely both elsewhere in the public sector, for example by local government and in the private sector, for example by shopping malls or residential buildings. Such uses of biometrics will raise the same issues as use by the police, especially as they are very often being used for a private policing purpose, except that any claim that the use is in the public interest will need more careful scrutiny where it is being done by those without a public mandate for policing to rely on. This

[15] See: https://www.adalovelaceinstitute.org/changing-the-data-governance-ecosystem-through-narratives-practices-and-regulations/

wider use has also led to a range of legal challenges across Europe.[16] In addition, we are all also now aware that the exploitation of our personal data for profit is built into the business plans of those who routinely harvest our data, from the global tech companies to the small online retailer.

THE PROBLEMS

My reason for pointing these things out is to illustrate how complicated creating a system of governance is going to be. We have allowed a new technology to rapidly develop across the fabric of our society without being clear about the implications and whether we wish to allow uncontrolled development. In part this is because of a fatalistic belief in technological determinism but also because, especially in this country we are remarkably careless with our civil liberties. We have allowed the development of CCTV coverage on a scale second only to that in China and the public response to that and police use of facial matching has been muted. Continental European countries have asked more searching questions and to them we owe the response of the GDPR and in the USA serious questioning has happened at both at state and federal level. Why this should be so I suspect is because we are the European country which escaped the Second World War horrors linked to invasion and state repression and because, unlike even most other common law jurisdictions, we are not citizens that have learned the meaning of citizenship from a founding constitution.

Many of the uses of the new technologies are either benign or are likely to be judged in some sense as in the public interest. In other words, the intrusion into our individual privacy may be acceptable when set against the benefits we derive. However, some uses of new technology may equally not be in the public interest nor justified by the benefits that we derive. Neither luddism nor allowing the private interests behind technology free reign are therefore sensible responses. That is why I now want to conclude by discussing two issues. First, the complications of legislating to govern the impacts of the new technologies and secondly, why addressing this issue will mean making a strategic political choice.

Some of the more detailed problems created by the new technologies might in fact be helped by the same technologies without the need for new governance. For example, the problem with AI-driven analytics is that it is not always clear how the end results were reached and therefore difficult to use evidentially in the criminal process - the so called ‘black box problem’. However, there is work currently going on to develop AI systems that can record how they reached their decisions. Solutions of this kind may reduce the problems but not do away with the main governance issues.

[16]For example, the Dutch Government's fraud algorithm SyRI breaks human rights, privacy law. See: https://www.dutchnews.nl/news/2020/02/governments-fraud-algorithm-syri-breaks-human-rights-privacy-law/ and in Sweden the data protection regulator has ruled against the use of facial recognition schools. See:https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/

LEGISLATING FOR NEW BIOMETRICS

The question of whether we should create a legislative framework for the new biometrics is not just being asked in England. The EU are asking the same question as are some States in the USA and to judge by the requests that I receive for interviews about the issue also many other countries. Leading the way in the development of legislation is however Scotland who already have a Bill to govern the police use of new biometrics in its final stages in the Scottish Parliament.[17]

Enacting such legislation is not easy and all countries are facing common problems. First, is how to respond to the speed of technical change? Legislators who seek to deal simply with a current concern, such as the police use of AFR, will quickly find that they are firefighting the next problem. A way has to be found to legislate for current **and future** uses of biometrics. Secondly, is the question of scale: should we seek to legislate for biometrics or more broadly for all AI-driven analytics? Thirdly, is the question of range: should legislation govern the police use of biometrics or should it extend to all public sector use or all use by anybody? These questions need to be decided before moving onto the technical problems of framing legislation.

Scotland's answer to these questions is to create legislation based on principles and then have a Scottish Biometrics Commissioner draw up an evolving code of practice for the use of biometrics based on those principles to govern the capture, retention, use and deletion of biometrics. Initially the code will apply to the police but with a possibility to later extend the range. The proposed Scottish Commissioner, as you can see has a very different role from mine. Because Scotland is the first country to legislate then it does offer a model for others but the particularities of the Scottish situation mean that it might not be a model that will easily fit England & Wales. Where Scotland **is** a model for all, is in the kind of questions that need to be addressed.

Carrying out this work will be especially difficult if governments wait until they are forced into rapid action by public concern. In Scotland they started with commissioning a report from a group of stakeholders and experts, consulted on their report, drafted legislation and consulted on those proposals before presenting a Bill to Parliament. This process took two years but has meant that broad agreement and support has been built for the proposals.

THE STRATEGIC CHOICE

However, deciding the future governance of biometrics involves a much larger strategic political choice about our future. The technological changes that will result from AI-driven analytics will

[17] Scottish Biometrics Commissioner Bill

transform much more than biometrics. What is happening is another one of those technically disruptive process which fundamentally change the social world. Politicians in democratic countries have been slow to understand that a new world is emerging outside their control.

However, that has not universally been the case and China recognised much more quickly the possibilities provided by new technologies, especially new biometrics, for social control, or as they interestingly refer to it for 'the rule of law': language can be slippery in debates about this problem. Because they see the possibilities they have also set themselves the goal of becoming world leaders in developing such technology. What is noteworthy about China's use of biometrics is that it goes beyond controlling and sanctioning people's actions, to changing the way people think about the nature of social order. Attempting to re-make both the social order and citizens thinking is clearly a politically strategic decision about what kind of world they regard as desirable. I mention what is happening in China not to shroud-wave the danger of a dystopian future. I doubt that the Chinese choice will appeal to us simply because of the centrality for us of individual's rights being a limitation on the exercise of politically organised social control. I mention the Chinese example only to illustrate the point that thinking about how the police should use new biometrics raise a bigger strategic question about what kind of political order and social world we wish to see come out of this new period of technological disruption?

In conclusion, as a society we are just emerging out of a period where technical change was regarded as inevitable to an understanding that some of the early products of the new technologies are of dubious value or in some cases positively harmful either to individuals or social life. As in earlier times of technological disruption, we can manage that process if we choose. Working out how to provide governance for the new technologies will be difficult since some of them operate beyond the nation state, although the state remains the source of law and a rules-based international system. Legislating for new biometric use by the police is a juridical problem but the primary question is what kind of social and political world do we want the new technology to create? It might not be easy to reach political agreement on that question but answering such questions is the point of politics. And the results of such debates is usually expressed through legislation which is why the American equivalent to the Today programme is called The Lawmakers.