JUSTICE SUB-COMMITTEE ON POLICING

FACIAL RECOGNITION: HOW POLICING IN SCOTLAND MAKES USE OF THIS TECHNOLOGY

WRITTEN SUBMISSION FROM ALISTAIR SLOAN, SOLICITOR

[1] This is a response to the call for views by the Justice Sub-Committee on Policing in respect of the use of facial recognition technologies in Scottish Policing. I am a Scottish solicitor practising in the field of information law; which includes both privacy and data protection law.

[2] I am going to confine my views to issues concerning privacy and data protection issues; including, the legal and regulatory basis under the current law and the current oversight, governance and transparency aspects of the use of facial recognition in policing in the context of data protection and privacy law.

[3] The use of facial recognition undoubtedly involves the processing personal data (indeed, in most cases, 'special category personal data') of individuals. There are a number of processing activities that take place other than the obvious one of running the image through facial recognition software; in particular, the collecting, storage, retrieval and eventual deletion of the image are all examples of processing activities concerning personal data.

[4] The current legislative provisions of most relevance in the present context is Directive (EU) 2016/680 ("The Law Enforcement Directive"), which is implemented in the United Kingdom through Part 3 of the Data Protection Act 2018. During the early stages of the creation of what is now Regulation 2016/ (the GDPR), it was decided to exclude processing of personal data by law enforcement bodies for the law enforcement purposes from the ambit of the GDPR. Instead, The Law Enforcement Directive was brought forward by the European Commission to provide a framework for the processing of personal data collected by law enforcement authorities for law enforcement purposes.¹

[5] Competent Authorities are those listed in Schedule 7 to the Data Protection Act 2018 and “any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.” [Data Protection Act 2018, section 30(1)]. Both the Chief Constables of the Police Service of Scotland and of the British Transport Police are listed as competent authorities in Schedule 7 (paragraphs 9 and 10 thereof respectively).

[6] The use of facial recognition by the Police Service of Scotland will fall within the ambit of the law enforcement purposes, defined in section 31 of the Data Protection Act 2018 as “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 safety.”

¹ The GDPR still applies to law enforcement agencies where they are processing personal data other than for the law enforcement purposes; for example, employment records in respect of their employees.
In short, the use of facial recognition technologies by Police Scotland would require to comply with the provisions of Part 3 of the Data Protection Act 2018; and in particular the six data protection principles in sections 35-40. In terms of section 34(3), the Chief Constable of the Police Service of Scotland (as controller) is not only required to comply with the data protection principles, but must also be able to demonstrate compliance with those principles. I would suggest that the section 34(3) duty is an important one for Parliament in its scrutiny. This is because the Chief Constable should be thinking about how he can demonstrate compliance with the data protection principles at the earliest stages. Therefore, the Chief Constable should be able to demonstrate to the Sub-Committee how Police Scotland is complying with those principles in respect of its current use of facial recognition technology and how it intends on complying with those principles in respect of its future use of facial recognition technology.

In addition to Part 3 of the Data Protection Act 2018, there is also Article 8 of the European Convention on Human Rights and Fundamental Freedoms, incorporated into our domestic law via the Human Rights Act 1998. Article 8 of course provides the right to a private and family life. The Police are a public authority for the purposes of the Human Rights Act 1998 and are therefore obliged to comply with that Act in their own right. Furthermore, the Courts, who will have to deal with any legal actions arising out of the use of facial recognition technology, are also a public authority for the purposes of the Human Rights Act 1998. Article 8 of the ECHR is engaged in respect of the use of facial recognition technologies.

The use of Automatic Facial Recognition (“AFR”) by the police has recently been the subject of an unsuccessful judicial review before the Queen's Bench Division (Administrative Court) of the High Court of Justice (England and Wales). In the matter of R (on the application of Bridges) v Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (hereafter “Bridges”) the Divisional Court considered the use of AFR technologies by the Chief Constable of South Wales Place. The judicial review challenged the use of AFR under both data protection and privacy law. The judgment contains some important information on how to apply data protection and privacy law to a technology, which, while intrusive, is of benefit to law enforcement agencies; such as the Police Service of Scotland. It should be noted that the Claimant in that case has sought permission to appeal to the Court of Appeal (England and Wales).

In Bridges, the court, unsurprisingly, concluded that the use of AFR interfered with the Claimant’s right to privacy under Article 8 of the European Convention on Human Rights and Fundamental Freedoms. In doing so, the court pointed out that AFR is significantly intrusive; in particular, “it goes much further than the simple taking of a photograph.” (para 54) The court also noted that biometric data (which includes photographs) is inherently private stating, “AFR technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances.” (Para 57). The speed

---

2 The Claim was based on the Data Protection Act 1998, rather than the Data Protection Act 2018. However, its analysis is still useful as the legislative schemes are sufficiently similar.
at which the data is erased does not preclude it from being an Article 8 interference: para 59

[11] Although the Bridges case was only dealing with AFR technologies, it is impossible to see how any use of facial recognition would not involve an interference with a person’s article 8 rights. The key questions are, then: (1) whether the use is in accordance with the law and (2) a proportionate means of pursuing a legitimate aim.

[12] In Bridges, the court concluded that, while there is an absence of specific legislation governing the use of facial recognition technologies; the framework in which South Wales Police were deploying the technology was sufficient. In particular, the court considered: the common law powers of the police to prevent and detect crime, the existence of primary legislation in respect of the processing of personal data and the internal policies of South Wales Police. The Court did note that the legislative framework would need to be reviewed periodically as the use of AFR increased.

[13] In terms of the use of facial recognition by Police Scotland going forward, the Scottish Biometric Commissioner Bill will have an impact and it will be necessary that the internal policies and procedures adopted by Police Scotland are clear and robust.

[14] The final ECHR compliance question (i.e. whether it is a proportionate means of pursuing a legitimate aim) is one that will need careful consideration in respect of each intended use of the technology. The very nature of the test means that a blanket “yes” or “no” cannot reasonably be provided. A clear Data Protection Impact Assessment (DPIA), perhaps multiple DPIAs, will be necessary. In my view, Police Scotland should already have been undertaking DPIAs in respect of this as part of the decision-making process.

[15] BC v Chief Constable of Police Service of Scotland [2018] CSOH 104 is another important decision to bear in mind; it, for the first time, declares that there is a right to privacy in the common law of Scotland. This declaration by the Lord Ordinary appears to go much further than the position in England and Wales, where the courts have resisted declaring the existence of a right to privacy at common law; instead, restricting it to the tort of ‘misuse of private information’. It is likely that the common law right of privacy will essentially mirror the GDPR, Data Protection Act 2018 and Article 8 of the ECHR, but its boundaries remain untested. Finally, that decision was made by a single Lord Ordinary sitting in the Outer House of the Court of Session and as such it is not binding. I am not aware that the decision has been reclaimed to

---

3 In the Bridges case, images taken which did not produce a match were immediately deleted. The Claimant fell into a category where his personal data was immediately deleted, as he was not on any wanted list. Although the biometric data was deleted instantly in cases where no match was made, the underlying CCTV footage was retained for a period of 31 days.

4 It is understood that the European Commission is presently in the early stages of planning bespoke legislation that will be aimed at the regulation of facial recognition technologies and other artificial intelligence technologies. This will, however, inevitably not become law until after the UK has left the EU.

5 DPIAs are required by the Data Protection Act 2018 (section 64) where the processing is of a kind likely to result in a high risk to the rights and freedoms of individuals. In my view the use of facial recognition technologies is a type of processing likely to pose a high risk to the rights and freedoms of individuals; therefore, a DPIA is a mandatory activity for Police Scotland. DPIAs are required before the processing begins.
the Inner House so it is unlikely to be considered there any time soon. Given its status in precedent, it will only be persuasive to Sheriffs and other judges in the Outer House. However, it is my view that Lord Brailsford’s decision is a well-reasoned one, which was ultimately inevitable when the court was asked to decide if such a common law right existed.

[16] The Sub-committee has asked about the use of facial recognition technology by private sector entities on behalf of Police Scotland. There are, of course, two ways in which private entities could be assisting Police Scotland here. Firstly, there are private entities contracted by Police Scotland who carry out activities for Police Scotland which involve the use of facial recognition technologies. Secondly, there are private sector organisations, which have in place their own facial recognition technologies and share information with Police Scotland, but not as part of a contractual arrangement with Police Scotland.

[17] Those organisations contracted by Police Scotland are in all probability going to be processors, as defined by section 59 of the Data Protection Act 2018. In this scenario, the Chief Constable would still be the “controller” and would continue to assume most of the responsibility and liability under the Data Protection Act 2018. Police Scotland is only permitted, by law, to use processors who “provide guarantees to implement appropriate technical and organisational measures that are sufficient to ensure that the processing will (a) meet the requirements of [Part 3 of the Data Protection Act 2018]; and (b) ensure the protection of the rights of the data subjects”.

[18] The law requires that the relationship between Controllers and processors be governed by a contract concluded in writing between the Controller and the Processor. That contract must cover a number of specific issues: (i) the subject-matter and the duration of the processing; (ii) the nature and purpose of the processing; (iii) the type of personal data concerned and the categories of data subjects involved; and (iv) the obligations and rights of the controller and processor.

[19] Processors are only entitled to act in accordance with the instructions of the controller. They cannot innovate on the processing; to do so would result in the processor becoming a joint controller with Police Scotland. Any processor who innovated on the processing would, in addition to becoming a controller, be unlawfully processing the personal data.

[20] The second category of private sector organisations are extremely unlikely to come within the ambit of Part 3 of the Data Protection Act 2018, but instead would be caught by the GDPR. Where the GDPR is applicable, the processing would concern special category personal data; the processing of which is prohibited unless the data subject has expressly consented to it or one of the conditions in Schedule 1 to the Data Protection Act 2018 applies.

[21] The legal regime in which Police Scotland operates with regard to facial recognition technology requires that the application of a test of strict necessity. That is, the processing of personal data in this way must be strictly necessary. This is a

---

6 Data Protection Act 2018, section 59(5).
7 Data Protection Act 2019, Section 59(6)(a).
high hurdle to cross, but not one that is impossible to get over (as Bridges demonstrates). DPIAs will assist Police Scotland in reaching conclusions about whether a particular use of facial recognition technology meets the test of strict necessity. For example, large-scale and long-term indiscriminate use of facial recognition technology is unlikely to meet the test of being strictly necessary. It is a matter that needs to be reviewed by Police Scotland ahead of each deployment and it may actually, depending upon the circumstances, be something that’s kept under review during the deployment.

[22] Section 49 of the Data Protection Act 2018 provides protections for individuals in respect of automated decision-making; in short, the law prohibits automated decision-making where it would result in a significant decision unless it is required by or authorised by law. A significant decision is one which produces an adverse legal effect concerning the data subject or significantly affects the data subject. An example of a significant decision would be a decision to arrest an individual; that significantly affects the data subject as it, at least temporarily, deprives them of their liberty.

[23] Police Scotland will also be required to produce an “Appropriate Policy document” where its use of facial recognition technologies relies upon any of the conditions for processing set out in Schedule 8 to the Data Protection Act 2018. Such a document is required to explain Police Scotland’s procedures for securing compliance with the data protection principles in connection with the sensitive processing and also explain the policies adopted by Police Scotland in relation to the retention and erasure giving an indication as to the length of time that the personal data in question will be retained.

[24] Transparency is a key aspect of the law relating to the protection of personal data. The Data Protection Act 2018 requires that certain information be provided to data subjects. These obligations are designed to ensure that processing of personal data is transparent; however, they are, of course, subject to certain exemptions. For example, where to provide the required information would prejudice an investigation, then the obligation to provide information can be appropriately restricted. Some uses of facial recognition technology can result in this being particularly difficult to achieve. An example of where providing the necessary information might present some difficulties would be a situation similar to the use in the bridges case. In those circumstances, Police Scotland would need to carefully consider to what extent it is required to provide such information and how it can best be provided (e.g. by displaying signs in an area subject to the use of facial recognition technology).

[25] The right of subject access is another way in which transparency is achieved. This right not only entitles data subjects to be provided with a copy their personal data being processed; but it also entitles them to be provided with a range of information by the controller. The right of subject access is not absolute and is subject to certain restrictions. Where a processor is involved in the processing, the

---

8 Data Protection Act 2018, section 44 – this information is contained in documents often known as "privacy notices".
9 In that case, South Wales Police were using AFR technology to scan a crowd in a public place (locations and events susceptible to criminality). The technology was capable of capturing up to 50 faces a second.
10 Data Protection Act 2018, section 45.
processor has specific obligations to assist the controller with responding to such requests.

[26] There is already a large amount of oversight in terms of Police Scotland’s use of facial recognition technology. The Information Commissioner is responsible for regulating and enforcing data protection law, including Part 3 of the Data Protection Act 2018. The Commissioner has various powers under that Act, including, dealing with complaints from data subjects; the power to conduct assessments; power to issue enforcement notices and powers in relation to the issuing of financial penalties. The courts also have oversight and affected data subjects have recourse to them in order to seek orders requiring controllers to comply with the law as well as seeking the award of damages. A petition to the supervisory jurisdiction of the Court of Session (judicial review) remains a viable option as well; in appropriate circumstances. Legal Aid is available for those who meet the financial and merits tests.

[27] The Scottish Biometrics Commissioner Bill, if enacted, will also provide for oversight by a new authority: the Scottish Biometric Commissioner. Images of an individual are within the ambit of the definition given to biometric data in section 23 of the Scottish Biometrics Commissioner Bill. Section 6 of that Bill provides for the creation of a code of practice in relation to the acquisition, retention, use and destruction of biometric data for criminal justice and police purposes. In terms of Section 7 of the Bill Police Scotland’s officers and staff will be required to have regard to the code. I assume that the code will include provisions relative to the use of facial recognition technology and therefore Police Scotland will have to have regard to those provisions when implementing facial recognition technology. This will provide an additional level of regulation and oversight in relation to the use of facial recognition technology by Police Scotland.

[28] The Scottish Police Authority has a general power to hold the Chief Constable to account for policing in Scotland. This would include decisions taken by, or on behalf of, the Chief Constable around the use of facial recognition technologies.

[29] Finally, while operational decisions are a matter for the Chief Constable, the Scottish Parliament can also exercise oversight in respect of those decisions and whether the Chief Constable is complying with their legal obligations about facial recognition technology. Indeed, this inquiry is an example of the Parliament’s oversight of Police Scotland on the issue.

[30] In terms of governance arrangements, there are various governance arrangements within the Data Protection Act 2018. I have already mentioned some of these (such as DPIAs and appropriate policy documents). There is the general accountability principle, which I have also mentioned elsewhere in this submission, requiring the Chief Constable to be able to demonstrate compliance with the data protection principles. The accountability principle will clearly require governance arrangements otherwise, the Chief Constable will be unable to demonstrate their compliance with the data protection principles.

---

11 Police and Fire Reform (Scotland) Act 2012, section 2(1)(e).
In addition to the Governance arrangements already mentioned, there are others (which I do not intend to go into in detail in any detail) such as records of processing activities.\footnote{Data Protection Act 2018, section 61.}

On 31 October 2019, the Information Commissioner issued her first opinion\footnote{https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf} given pursuant to section 116(2) of the Data Protection Act 2018. This Opinion relates to the use of live facial recognition technology by law enforcement in public places. The Opinion considers the judgment in 
\textit{Bridges} (in which the Commissioner intervened as an interested party). The Commissioner expresses her view\footnote{Information Commissioner’s Opinion: The use of live facial recognition technology by law enforcement in public places, 31st October 2019, Reference: 2019/01 at page 9.} that there should be a binding statutory code of practice be issued by the Government. I have already indicated my assumption that the code of practice set out within the Scottish Biometrics Commissioner Bill would cover the use of facial recognition technology by the police. The Commissioner’s recommendation goes further. Firstly, the Scottish Biometrics Commissioner Bill only requires that Police Scotland’s officers and staff have regard to the code of practice. The Courts are consider whether it has been complied with, but the Bill makes it clear that there is no right of legal action created in respect of a failure to comply with the code of practice.

The code within the Scottish Biometrics Commissioner Bill does not appear to me to go as far as suggested by the Commissioner. It is not going to be binding upon Police Scotland. The Scottish Biometrics Commissioner Bill is of course currently being considered by the full Justice Committee; however, there is an inevitable overlap between that Bill and the issues being considered by the Justice Sub-Committee as part of this inquiry.

The Commissioner in her Opinion suggests that “[s]uch a code should provide greater clarity about proportionality, given the privacy intrusion that arises as a result of the use of LFR, eg facial matching at scale. Without this, we are likely to continue to see inconsistency across police force and other law enforcement organisations in terms of necessity and proportionality determinations relating to the processing of personal data. Such inconsistency, when left unchecked, will undermine public confidence in its use and lead to the law becoming less clear and predictable in the public’s mind.”\footnote{Ibid, page 10.} It appears that the Commissioner envisages a UK-wide code issued by the UK Government. A unified code, if it can be achieved, would be of assistance to the public and law enforcement agencies; however, it may come into conflict with the provisions within the Scottish Biometrics Commissioner Bill.

The Commissioner has indicated at the end of her Opinion a number of steps that she intends to take. Those include issuing a further Opinion on the use of live facial recognition technologies by the private sector; including those who work collaboratively with the police and other law enforcement agencies. This Opinion might well have some impact upon controller-processor relationships that Police Scotland develop in respect of the use of facial recognition technology. This would be a welcomed development as the Committee will appreciate that private sector
organisations acting as processors for Police Scotland work within different confines and will have different considerations from the controller.

[36] I hope that this submission will be of assistance to the sub-committee. If the Committee would like further information, I would be happy to provide that in writing or at an oral evidence session.

Alistair Sloan
Inksters Solicitors
October 2019