Law Society of Scotland

Consultation Response

Consultation on enhanced oversight of biometric data for justice and community safety purposes

October 2018

Introduction

The Law Society of Scotland is the professional body for over 11,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders and our membership.

Our Criminal Law Committee together with our Privacy Law Sub-committee, welcomes the opportunity to consider and respond to the Scottish Government's *consultation on enhanced oversight of biometric data for justice and community safety purposes*.[1]

We fully support the intention to bring forward legislation in relation to biometric data. 'Biometric data' must be clearly defined so that the scope of the legislation can understood by the public and all those required to apply the rules in the Code of Practice governing acquisition, use, retention and disposal. For instance, biometric data is defined in the Data Protection Act 2018 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"[2]. It is important that there is consistency use of the term 'biometric data' across legislation in so far as is practicable. The proposal to appoint a Scottish Biometric Commissioner is a much-needed appointment in relation to the oversight of such data.

We highlight concerns around the interaction between safeguarding the privacy of individuals and the identification and prevention of crime. A balance must be achieved: proportionality is key to ensuring that challenges to forthcoming legislation are kept to a minimum.

[1] https://consult.gov.scot/safer-communities/use-of-biometric-data/

[2] Section 205

General remarks

We welcome consideration of the acquisition, use, retention and disposal of biometric data. The consultation takes forward certain recommendations made in the Report by the Independent Advisory Group (IAG) on the Use of Biometric Data in Scotland[3] (IAG Report). Since the consultation commenced, the Scottish Government has also announced its intention to introduce a Biometric Data Bill as part of its Programme for Government 2018-2019.[4] We support the introduction of a statutory Code of Practice to cover biometric data and technologies and the appointment of a Scottish Biometrics Commissioner.

As is recognised, the term 'biometric data' must be carefully defined. This is essential, and we recognise that it may prove challenging. Without a clear statutory definition, the scope of the proposed Bill will be uncertain and open to challenge. The IAG Report defined 'biometric data' as 'any physical, biological, physiological or behavioural data from human subjects which will have the potential to identify another[5] individual'[6]. Whether that is the appropriate definition is a matter for drafting at the relevant time, but we also note that it is essential that the legislation can be future-proofed.[7]

Developments around biometric data are fast-moving so the definition of biometric data must take account of advice from appropriate experts to produce a definition that is relevant today but will also encompass future advances in these relevant technologies. The legislation must be wide enough to ensure all relevant data is caught and subject to the Code of Practice and the remit of the Scottish Biometrics Commissioner. Biometric data has a meaning within both the justice and community safety context in Scotland.

Biometric data has a wider use within the justice system which is not confined merely to its criminal application. There is only a tacit reference in the consultation to its wider use within a disaster where there may be a need to identify individuals.[8] The acquisition and retention of data may well need to be subject to the same considerations as are being set out within the consultation.

It is also important to ensure consistency with other legislation. The Counter-Terrorism and Border Security Bill[9] is currently proceeding through the UK Parliament. There are references within the Bill's Schedule 2

[3] https://beta.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/pages/1/

4 https://beta.gov.scot/programme-for-government/

5 This has been changed in the draft Code of Practice to 'known' from 'another.' The word 'known' may well raise questions as to whom the person is 'known'.

6 Paragraph 1.7 of the IAG Report

7 Paragraph 6. Of the Consultation

8 The role of the COPFS in relation to reporting of deaths might be useful to consider – see further http://www.copfs.gov.uk/images/Documents/Deaths/Reporting%20Deaths%20to%20the%20Procurator%20Fiscal%202015.pdf

9 https://services.parliament.uk/bills/2017-19/counterterrorismandbordersecurity.html

as introduced to the retention[10] of biometric data for counter-terrorism purposes. The scope of the meaning of biometric data also needs to be consistent across the UK as do the standards and good practices.

The public need to have confidence in the gathering, use and storage of biometric data. Any retention of biometric data will potentially present a risk as it may well be vulnerable to mishandling and abuse. However, collection of information is clearly essential for prevention, detection and prosecution of crime.

The real issue as identified by Baroness Hale is:

"whether keeping the information… is "necessary in a democratic society" in the sense in which that phrase is now understood: is the means used, and the interference with privacy which it involves, a proportionate way of achieving those legitimate aims? In particular, is it proportionate to keep the information...in the form in which it was kept, and for the length of time for which it was kept? These are not easy judgments to make. If society can trust the police to behave properly, and not therefore to misuse the information which they have, there is much to be said for allowing the police to keep any information which they reasonably believe may be useful in preventing or detecting crime in the future."[11]

The stress would be on ensuring that there is transparency about the acquisition retention and use of such data as well as ensuring that there are safeguards to minimise breaches and against the misuse of such data. International press coverage shows the vulnerability to data breaches that arise now such as in the USA where 1.1milion fingerprints were stolen.[12]

Response

Question 1: Do you believe a statutory Code of Practice covering the acquisition, use, retention and disposal of biometric data for justice and community safety purposes is required?

Yes. There are a number of reasons why a statutory Code of Practice should be put in place. The Criminal Procedure (Scotland) Act 1995 (1995 Act) already sets out the procedures governing the obtaining of biometric samples such as fingerprints as well as the rules for its retention and use. It is important that any Code of Practice should not seek to change the existing law.[13] It should consolidate the current law as changes are made to take account of new procedures and techniques as set out in the future Bill.

A Code of Practice provides an opportunity to set out:

10 Paragraphs 6-17 of the Counter-Terrorism and Border Security Bill

11 *R (on the application of Catt) (AP) (Respondent Commissioner of Police of the Metropolis a another (Appellants)* [2015] UKSC 9

12 https://findbiometrics.com/opm-data-breach-27101/

13 Paragraph 16 of the consultation

- the scope of its application to safeguard the public interest;
- the extent of the biometric data it covers; and
- the organisations affected and required to comply.

By addressing these issues, it should provide in an easily understood and comprehensive fashion for the public a 'one stop shop'. It will serve both those who require to adhere to its standards as well as those affected by the use and retention of such data. The publicity surrounding the launch of a Code of Practice will have benefits of enhancing public awareness as to the powers and provisions as well as promoting much needed transparency of the way that such data will be handled.

The consultation has usefully set out in detail the types of data which fall within the scope of the Code of Practice. We would be interested with reference to our comments on the proposed definition of biometric data how 'first generation' and 'second generation' biometrics are to be defined.[14]

Question 2: Do you believe the proposed statutory Code of Practice is being applied to the correct individuals/agencies?

The consultation sets the categories of bodies to which the code applies:

1. those to whom the Code applies on a statutory basis (Police Scotland and the Scottish Police Authority);
2. public authorities on a voluntary basis;
3. the private sector when carrying out work on behalf of, or feeding into the work of, bodies to whom the Code applies.

As far as Police Scotland is concerned, the consultation seems to envisage a period of grace when voluntary compliance would ensue prior to the Code of Practice's formal adoption. There seems to be a division too in the way that the functions of Police Scotland would be governed. This depends on whether it is operating under the instructions of the Crown Office and Procurator Fiscal Service (COPFS). COPFS will only be involved when a report is made to them or in a murder where they are in charge at the outset in directing proceedings. We note that there may well be biometric data obtained at the outset of the investigation before there is any report to COPFS. There is a question as to whether this would make a technical difference.

Into which group each organisation may fall could be complicated. Is a school a private organisation or a public one in that the public has a right of access? Is a train station a public organisation? There should be consistency so that all agencies who can legitimately acquire, retain, use or dispose of biometric data for justice and community safety purposes in Scotland are required to adhere to the Code of Practice.

We note in terms of paragraph 20 of the consultation that treatment of biometric data which is obtained under national security grounds is reserved and not under the competence of the Scottish Government.

[14] Paragraph 7 of the draft Code of Practice

National security is a reserved matter but in criminal law, the procedures and organisations involved will be governed by Scots law. That should not pose significant issues, but we would highlight various areas which would need to be clarified as the Bill is drafted:

- Consideration will require to be made of the Counter-Terrorism and Border Security Bill referred to above. Account needs to be taken of the current progress of that UK Bill which does refer to how samples are collected and retained. It does refer specially to Scottish procedure and to the 1995 Act regarding collection of such data.

- A Commissioner for the retention and use of biometric material in England and Wales already exists. Envisaging that the appointment of a Scottish Biometric Commissioner will be made, clarification of the extent of their remit will need to be considered. Biometric data obtained on national security grounds will presumably continue to be the responsibility of the Biometrics Commissioner and include Scotland. Will the Scottish Commissioner have any oversight in relation to such data? We note that The Biometrics Commissioner indicates at present that:

  "The role of the Biometrics Commissioner was established by the Protection of Freedoms Act 2012... His role is to provide independent oversight of the regime which was established by PoFA – and which came into force on 31 October 2013 – to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints."[15]

This is important today given the role of terrorism and concerns relating to national security and the cross-border nature of serious organised crime. We would encourage clear information to be available on the websites of both commissioners.

We also consider that further clarification is required regarding the status of the Code of Practice when it is being applied on a voluntary basis by, for example, public authorities and the private sector. The question which arises is whether, once an organisation adopts the Code of Practice on a voluntary basis, adherence to it thereafter becomes mandatory. It may also be helpful to consider whether the Code of Practice could be adopted in part or must be adopted in its entirety. Clarity on this would be valuable for both organisations and data subjects. An analogy might be drawn with the role of Data Protection Officers (DPO) under the General Data Protection Regulation (GDPR), where an organisation which does not require a DPO can choose to have one. If it does so, then that will be a statutory DPO and bound to meet all the corresponding duties.

Additional clarification may be needed in relation to paragraph 16 of the Guidance and the private sector/law enforcement interface.

15 https://www.gov.uk/government/news/biometrics-commissioners-fourth-annual-report-2017

Question 3: Do you believe the General principles outlined in the statutory Code of Practice are the right ones?

We support the General principles set out in the statutory Code of Practice.

However, these must be extended to include specific reference to security, which is of particular concern in relation to data being obtained of such a sensitive nature. As we highlighted above, it is almost inevitable that there will be breaches: the need for robust security measures should be highlighted and enforced as a matter of paramount importance.

We appreciate that much of the Code of Practice reflects current procedure. Publication of a Code of Practice provides an opportunity to emphasise the need for security to be observed to reduce the risks of breaches arising to the detriment of public confidence. It is important to recognise that if there is a breach of data such as a telephone number, this can be changed. If biometric data is lost, it is not possible to change it in the same way. The consequences may therefore be considerably greater. Enhancing the requirement for security can be undertaken without compromising the functionality and use or acquisition of biometric data.

Question 4: Do you believe that the statutory Code of Practice covers all relevant issues which require consideration when decisions are being taken about the acquisition use retention and disposal of biometric data?

The Code of Practice is wide and detailed which we support. There is a need to ensure that the Code of Practice is also future-proofed and retains sufficient operational flexibility, so it would not need to be frequently revised and updated in the light of technological and scientific advances. (See paragraph 41).

We would make a number of observations on the Code:

Paragraph 6 and 7: There is, as we have emphasised above, a need to define consistently what is meant by biometric data and therefore the scope of any Code of Practice to be applied. The definition in the Code of Practice is described as encompassing first and second-generation biometrics. However, it goes on to refer to data obtained in other non-policing public sector contexts.[16] We are unsure that the public at large would necessarily understand the scope of the term 'biometric data', which could cause difficulties including, for instance, comprehension by juries. There may be scope for the production of simple guides such as those developed for the judiciary, which set out the scientific background on topics such as DNA in accessible terms.[17]

[16] Paragraph 7 of the consultation

[17] See, for instance, https://royalsociety.org/news/2017/11/royal-society-launches-courtroom-science-primers/

Paragraph 10: We are interested in how compliance of the Code of Practice is to be promoted by proposed Scottish Biometrics Commissioner.

Paragraph 12: The Code of Practice is not to affect existing law. This is an opportunity to make sure that the existing law and practices are clearly understood.

Paragraph 15: We question if this includes all the relevant organisations.

Paragraph 30: This refers to the legacy custody systems and historic data. There needs to be adequate protection from accessing then in future. We note that paragraph 30 says that:

"In relation to custody images held by Police Scotland on legacy force custody systems where there is no automated means of distinguishing between records of convicted and non-convicted persons, it will suffice for the records within those systems to be protected from access in the operational environment until deleted as those systems are shut down. Subject to this caveat on historic images within legacy force systems, it is necessary to ensure that biometric data is completely expunged in circumstances where there are no longer legal grounds for retaining the data in question."

It must be recognised that indefinite retention of records of convicted and non-convicted persons without a specified, explicit legitimate purpose has never been legal.

We also have the following comments on the text:

- Further clarity is needed regarding the meaning of "protected from access in the operational environment".
- "as those systems are shut down": The text refers to systems being shut down but does not set out what should happen to the data in those systems. Will it be deleted or retained elsewhere as appropriate?
- " …no longer legal grounds for retaining the data in question" Greater clarity on retention periods is needed to ensure consistency and transparency for data subjects.

Part 3- 'General Principles' and ethical considerations

Paragraphs 43, 45 and 47: Under the General Principles, we consider that the aspect of security should be clearly articulated.

Part 4- privacy by design

There is a need to ensure that the requirements of data protection legislation with respect to privacy by design are fully respected. This section is helpful as far as it goes. We consider that it may also be appropriate to develop, for consistency, a standard procedure for carrying out Data Protection Impact Assessments.

Part 6- Biometric data review and appeals process

Paragraph 64: We fully support that there should be a clear appeal process for those persons who consider that there have been breaches of the acquisition, use or retention of their personal data. These rights must not usurp any rights that are available under the relevant data protection or other legislation.

Paragraph 84: There is a reference to Improvement Notices being served. Exactly how that process should work should be clearly set out.

Question 5 Do you believe a Scottish Biometrics Commissioner is required?

Yes. We fully support the creation of a Scottish Biometrics Commissioner. There is a Commissioner for England and Wales whose role is to provide oversight and decision-making powers about the retention and use of biometrics. The remit is UK-wide but for criminal matters is only for England and Wales.

Exactly how the interaction or overlap between the two roles is to operate will need to be sorted out. Criminal matters correctly fall within devolved matters and need to take account of the Scottish-specific landscape. There does need to be consistency across the UK in practices, particularly given the international dimension to crimes especially in the field of terrorism and serious organised crime.

Question 6: Do you believe the Commissioner's statutory remit extends to the correct individuals /agencies?

Yes.

Question 7: Do you believe the proposed general functions of the Scottish Biometric Commissioner are the right ones?

Yes.

Question 8: Do you believe the proposed approach to the acquisition of biometric data from children and young person in the justice system is the right one?

There is a need to ensure consistency with the Age of Criminal Responsibility (Scotland) Bill which is currently proceeding through the Scottish Parliament. It deals too with the acquisition and retention of biometric data.

Question 9: Do you have any views on the appointment and accountability arrangements for the Commissioner?

We endorse the consultation's recognition of the need for transparency in the appointment process.

For further information, please contact:
Gillian Mawdsley
Policy Team
Law Society of Scotland
DD: 0131 476 8206
GillianMawdsley@lawscot.org.uk