HOUSE OF COMMONS LIBRARY

DEBATE PACK

Number CDP 2019/0099, 30 April 2019

Facial recognition and the biometrics strategy

By Jennifer Brown
Georgina Hutton
Hannah Wilkins
John Woodhouse
Alison Pratt

Summary

This House of Commons Library debate pack has been prepared in advance of a debate entitled “Facial recognition and the biometrics strategy”. This will be led by Darren Jones MP and will take place on Wednesday 1 May 2019 in Westminster Hall, starting at 2.30 pm.

The Home Office published its *Biometrics Strategy* in June 2018. This sets out how the Home Office and its partners currently use biometric data, and how they will approach its use in future. According to the Strategy, the Home Office will:

- Deliver biometric services designed to be shared and re-used ensuring privacy is addressed in their design and development
- Make it possible to integrate different Home Office fingerprint services to streamline processes and produce quicker, cheaper and more accurate responses for immigration and policing purposes
- Seize opportunities to use biometrics across the criminal justice system to verify identity and identify individuals
- Use facial matching to verify more accurately individuals at ports ofeEntry
- Improve the automation of fingerprint enrolment at visa application centres to fix and verify identities of foreign nationals applying for visas to come to the UK
- Enable more efficient review and automatic deletion of custody images by linking them to conviction status, more closely replicating the arrangements for fingerprints and DNA
- Consider the case for sharing and matching of facial images held by the Home Office sector and those of other government departments

This debate pack provides background information on some of the areas covered by the Strategy, as well as parliamentary material, press articles, and further reading which Members may find useful when preparing for the debate.

Contents

The House of Commons Library prepares a briefing in hard copy and/or online for most non-legislative debates in the Chamber and Westminster Hall other than half-hour debates. Debate Packs are produced quickly after the announcement of parliamentary business. They are intended to provide a summary or overview of the issue being debated and identify relevant briefings and useful documents, including press and parliamentary material. More detailed briefing can be prepared for Members on request to the Library.

www.parliament.uk/commons-library | intranet.parliament.uk/commons-library | papers@parliament.uk | @commonslibrary

1. Background

1.1 Biometrics

Biometric technologies identify individuals based on distinguishing physical and behavioural attributes, such as fingerprints, face, iris, voice and DNA. Automated biometric systems are pattern matching systems that match input biometric data against one or more reference records (either a database or a single record, such as a passport). They are used in two main ways:

- Verifying a persons' identity by comparing a biometric attribute against a reference record (e.g. matching a person's face against their passport)
- Identifying a person by comparing a biometric attribute against a set of reference records of many people (e.g. matching a fingerprint collected at a crime scene against a database of previous offenders).

A June 2018 POST note on biometric technologies provides more information about the technology. Section 1.2, page 6 below lists national databases that hold biometric data.

The most established biometric attributed used are fingerprints, DNA and face – these are the only biometric attributes included in the Biometrics Strategy. Newer biometric technologies are being developed using voice, or behavioural characteristics such as gait.

Most biometric systems are probabilistic and therefore involve some degree of error. A key consideration is the threshold set for accepting a match.[1] A high threshold will lead to fewer false matches but more false non-matches (failures to identify a genuine match), and vice versa. The threshold chosen depends on the application. For example, high security situations (e.g. passport control) may set a higher threshold to reduce someone being falsely admitted. Less secure applications may set a lower threshold to minimise the inconvenience of false rejections.

Facial recognition

The Biometrics Strategy refers to two types of facial recognition – facial matching and automated facial recognition:

- *Facial Matching* matches a facial image, sometimes referred to as the 'probe' image, against either a single image, such as that held on a passport (1-to-1), or a database of images taken in controlled environments (1-to-many). An example would be the checking of an image of a suspect against images of persons taken on arrest.
- *Automatic Facial Recognition (AFR)* is the checking of facial images, generally obtained in an uncontrolled public environment, against a watch list of people whose images

[1] POSTnote, Biometric Technologies, 29 June 2018, Box 2.

> have been taken in controlled or uncontrolled environments.[2]

Automated Facial Recognition can be used to identify people against a watch list using real time surveillance footage such as CCTV. Both the Metropolitan Police and South Wales Police are running trials attempting to match some retained facial images with people in public places (see Section 1.2 page 8 below).[3]

The Commissioner for the Retention and Use of Biometric Material in his Annual Report 2017 stated that there is good evidence for matching capabilities of facial recognition technology for controlled use environments but that there is little evidence about matching in more challenging automated facial recognition applications. For the latter, carefully designed trials could prove useful:[4]

> Whilst there is good evidence of the matching capabilities of different facial matching software products in reasonably controlled use environments, such as matching custody images or passports at airports, there is little evidence as yet about matching for this much more challenging use. Furthermore, what needs to be understood is not just the matching capabilities of the software products but what kind of management and decision making system is required for such a police use in the criminal justice system. In this context trials can be justified if they have been carefully designed to provide new evidence to fill these gaps in knowledge and the results of the trials are published and externally peer reviewed. Crucially, there needs to be transparency about the reason for conducting trials and, in particular, what safeguards are built in to protect personal biometric data as well as consideration of the proportionality of its use.

Accuracy and bias

The Government Office for Science Biometrics guide (June 2018) states that the accuracy of facial recognition is variable. The guide states that then recent best figures (based on optimal conditions) have an Equal Error Rate[5] of 0.2%, however errors for low-resolution surveillance footage can exceed 10%.[6] Factors that affect accuracy include the quality of the images, differences in lighting and image view angle.

Some studies have found that some facial recognition algorithms can be less good at recognising certain groups, for example ethnic groups, age groups or gender.[7] One reason for this is when training/reference data used to develop the algorithm is not sufficiently diverse. The Government Office for Science biometrics guide says that some research

[2] Home Office, Biometrics Strategy, 28 June 2018, page 11.

[3] Commissioner for the Retention and Use of Biometric Material, Annual Report 2017, March 2018, para 308.

[4] Commissioner for the Retention and Use of Biometric Material, Annual Report 2017, March 2018, para 308.

[5] Equal Error Rate is the value where the proportion of false positives is equal to the proportion of false negatives.

[6] Government Office for Science, Biometrics: a guide, 15 June 2018, page 6.

[7] See: POSTnote, Biometric Technologies, 29 June 2018, page 6; and Government Office for Science, Biometrics: a guide, 15 June 2018, page 6 and underlying references.

suggests that no algorithm will ever perform ideally for everyone, with some users being prone to misidentification.[8]

1.2 Police

The police have wide ranging powers to collect and retain the biometric data of those they suspect have committed a crime. The police frequently use biometric evidence to assist in their investigations.

The Biometric Strategy contains two main initiatives relevant to the police. Both of which concern the use of facial recognition data:

- The establishing a new oversight and advisory board for their use of facial recognition.[9]
- Continuing to implement the findings of the 2017 Custody Image Review.[10]

In addition to these key improvements to police use of facial recognition data, the strategy pledges to continue to uphold and improve the standards for the use of DNA and fingerprint data by the police.

Legislation

Part V of the *Police and Criminal Evidence Act 1984* (known commonly as PACE) is the primary piece of legislation which governs the use of biometrics by the police. However, there are a number of other statues which contain relevant provisions (as set out in the annex of the Home Office's Biometrics Strategy). The Home Office maintains a set of codes to compliment PACE, PACE code D provides guidance on the methods of identification used by the police and covers the use of biometrics.

Using PACE powers, the police normally take a photograph, the fingerprint information and a DNA sample from every individual they arrest.[11] These records are then then checked against national databases to see if the person can be linked to an unsolved crime.[12]

Section 61 of PACE provides the police with powers to take a person's **fingerprint** information without their consent if they have been arrested, charged or bailed for a "recordable offence" (i.e. will be recorded in national police records).[13]

Section 64A of PACE provides the police with powers to take the **photograph** of anyone who is detained at a police station with or without their consent.[14]

The legislation creates a distinction between 'intimate' and 'non-intimate' **DNA evidence**. 'Intimate' DNA includes (but is not limited to)

[8] Government Office for Science, Biometrics: a guide, 15 June 2018, page 6.

[9] Home Office, Biometrics Strategy Better public services: Maintaining public trust, June 2018,, paragraph 42

[10] Ibid, paragraph 32 and 33

[11] P7

[12] Ibid

[13] Home Office, PACE Code D, February 2017, part 4.

[14] s64A(4), *Police and Criminal Evidence Act 1984*

blood and urine samples. 'Non-intimate' DNA includes (but not limited to) most hair follicles and salvia samples.[15]

Section 62 allows the police to take an 'intimate' DNA sample from a person in police detention only if an officer of or above the rank of inspector deems it necessary and the suspect has given consent. Suspects are warned that if they withhold their consent their refusal may harm their case if it comes to trial.[16]

Section 63 allows the police to take a 'non-intimate' DNA sample without consent if the individual has been arrested, charged, bailed or convicted for a "recordable offence".[17]

National Databases

There are four main databases which hold biometric data obtained by the police:

- The National DNA Database (NDNAD)
- The National Fingerprint Database (IDENT 1) which holds fingerprint information.
- The Police National Computer (PNC) and the Police National Database (PND). Where custody photos and other identifying images stored locally are shared between police forces.

The DNA and fingerprint information of people who have been convicted of a crime are held indefinitely. Individuals who have not convicted of a crime may have their information held for up to five years depending on the circumstances.[18] This 'retention schedule' is dependent on provisions in the *Protection of Freedom Act 2012*. Depending on certain criteria, individuals may be able to apply for the early deletion of their records.[19]

National databases in numbers

The **NDNAD**:

- Holds the DNA of an estimated **5.37 million** people.[20]
- In 2017/18 records relating to **38 thousand** crime scenes were uploaded.[21]
- In 2017/18 there were **30,780** routine 'subjects to crime scene' matches including **716** homicides and attempted murders **694** rapes.[22]

The **IDENT 1** Holds fingerprint records on around **8 million** individuals.[23]

Oversight

Police use of biometric data is overseen by several independent public bodies:

[15] Home Office, PACE Code D, February 2017, section 6.1
[16] Ibid, section 6.3(b)
[17] Home Office, PACE Code D, February 2017, section 6.6.
[18] ACRO, Retention Schedule, [last accessed 25/04/19]
[19] ACRO, Deletion of records from national police systems [last accessed 25/04/19]
[20] NPCC and the Home Office, National DNA Database Strategy Board Annual Report 2017/18, February 2019, p10
[21] Ibid, p11
[22] Ibid, p17
[23] Ibid, P38

- The Forensic Science Regulator monitors and maintains standards in forensic science services across the criminal justice system. The Government is supporting a Private Members Bill (Forensic Science Regulator Bill 2017-19) to give the regulator statutory powers of enforcement. This forms part of their 13-point action plan to improve the quality of police forensics.
- The Biometrics Commissioner keeps under review the retention and use of DNA and fingerprints by the police.
- The Information Commissioner's Office (ICO) upholds information rights in the public interest, including where it relates to the police.
- The Surveillance Camera Commissioner promotes compliance with the surveillance camera code of practice.
- The NDNAD Strategy Board provides governance and oversight of the NDNAD and the IDENT 1. It is chaired by a senior police officer and is comprised of representatives from the police, the Home Office and the above oversight bodies.

ICO concerns about facial recognition technology

Elizabeth Denham, the Information Commissioner, raised concerns about facial recognition technology and law enforcement in a blog of 14 May 2018 (before the GDPR and 2018 Act came into force):

> (…) how facial recognition technology [FRT] is used in public spaces can be particularly intrusive. It's a real step change in the way law-abiding people are monitored as they go about their daily lives. There is a lack of transparency about its use and is a real risk that the public safety benefits derived from the use of FRT will not be gained if public trust is not addressed.
>
> A robust response to the many unanswered questions around FRT is vital to gain this trust. How does the use of FRT in this way comply with the law? How effective and accurate is the technology? How do forces guard against bias? What protections are there for people that are of no interest to the police? How do the systems guard against false positives and the negative impact of them?
>
> At another level, I have been deeply concerned about the absence of national level co-ordination in assessing the privacy risks and a comprehensive governance framework to oversee FRT deployment. I therefore welcome Baroness Williams' recent confirmation of the establishment of an oversight panel which I, alongside the Biometrics Commissioner and the Surveillance Camera Commissioner (SCC), will be a member of.
>
> I also welcome the recent appointment of a National Police Chiefs Council (NPCC) lead for the governance of the use of FRT technology in public spaces.
>
> A key component of any FRT system is the underlying database of images the system matches to. The use of images collected when individuals are taken into custody is of concern; there are over 19 million images in the Police National Database (PND) database. I am also considering the transparency and proportionality of retaining these photographs as a separate issue, particularly for those arrested but not charged for certain offences. The Biometrics Commissioner has also raised these concerns.
>
> For the use of FRT to be legal, the police forces must have clear evidence to demonstrate that the use of FRT in public spaces is

> effective in resolving the problem that it aims to address, and that no less intrusive technology or methods are available to address that problem. Strengthened data protection rules coming into law next week require organisations to assess the risks of using new and intrusive technologies, particularly involving biometric data, in a data protection impact and provide it to my office when the risks are difficult to address...[24]

According to December 2018 press reports, the ICO is investigating the use of facial recognition technology.[25]

Initiatives in the strategy

Facial recognition

The Strategy notes that unlike fingerprint and DNA samples, for which the NDNAD Strategy Board provides oversight, there is no specific oversight body for facial recognition data. The Strategy therefore proposes the creation of a new oversight and advisory body to coordinate and consider issues relating to the police's use of facial images and facial recognition systems.[26]

Like the NDNAD Strategy Board, the new body will be comprised of representatives from the police, the Home Office and all the existing oversight bodies. It will consider issues such as the policies for retention, deletion and use of facial images and whether police guidance and practices are compliant with legislation.[27]

The strategy also notes a desire to explore the use of new 'automatic facial recognition' (AFR) technologies by the police for crime investigation and prevention. For example, the strategy notes the use of AFR in South Wales:

> South Wales Police have used AFR to compare images of people in crowds attending major public events such as concerts, with pre-determined watch lists of suspected mobile phone thieves. Watch lists, created for time limited and specific purposes, could also include individuals banned from attending an event or known criminals who have previously operated in crowded spaces.[28]

Custody Image Review

The Home Office published a Review of the Use and Retention of Custody Images in February 2017. This review was promoted by a High Court case which found the practice of retaining the images of un-convicted individuals unlawful.[29]

Photographs taken of individuals upon arrest are held locally by individual forces and uploaded to the Police National Database (PND) and sometimes the Police National Computer (PNC). The Review

[24] Elizabeth Denham, "Facial recognition technology and law enforcement", ICO Blog, 14 May 2018

[25] "Britain's data commissioner launches investigation into UK use of facial recognition", Telegraph, 3 December 2018

[26] Home Office, Biometrics Strategy Better public services: Maintaining public trust, June 2018, paragraph 42

[27] Ibid, paragraph 43

[28] Ibid, paragraph 36

[29] [2012] EWHC 1681

proposed the introduction of a facility for individuals who are released without charge or acquitted at trial, to apply to have their photograph removed from police records.[30] This would bring the policy of retention of photographic evidence of un-convicted individuals more in line with that of the retention of DNA and fingerprint information.

To support the implementation of the Review the College of Policing issued updated Authorised Professional Practice guidance to police forces on the retention, review and disposal of custody images. This document provides advice to police forces on how they should review images, decide whether they should be retained and process requests for their deletion.

The Biometric Strategy commits to support the implementation of the Custody Image Review. It states that better technology will be introduced to automatically prompt the review of custody images on the PNC and the PND by linking data on conviction status.[31]

1.3 Immigration

The use of biometric data has been standard for UK immigration purposes for some time. Biometric information is used to facilitate the movement of visitors, migrants and British citizens through the UK border, and as part of UKVI visa applications. Biometric immigration documents were introduced in 2008 as evidence of the holder's immigration permission.

Legislative framework

Powers under the *UK Borders Act* 2007 allow the Home Office to issue 'biometric immigration documents' which are the biometric residence permit (BRP) and the short stay permit (SSP). The following regulations set out the legal basis for taking biometric information from applicants:

- Immigration (Biometric Registration) Regulations 2008 for biometric immigration documents
- British Nationality (General) (Amendment) Regulations 2003 (as amended) for naturalisation
- The Immigration (Provision of Physical Data) Regulations 2006 (as amended) for non-EEA citizens entitled to EU free movement rights or under any provisions made under s2(2) of the European Communities Act 1972

The definition of biometric information for immigration purposes is set out in s15 of the *UK Borders Act* 2007 (as amended by the *Immigration Act* 2014). It includes predominantly 'information about a person's external physical characteristics including in particular fingerprints and features of the iris'.

Biometric immigration documents and passports

[30] Home Office, Review of the Use and Retention of Custody Images, February 2017, paragraph 1.7

[31] Home Office, Biometrics Strategy Better public services: Maintaining public trust, June 2018, paragraph 33

Biometric British passports (commonly referred to as "e-passports" were first introduced in 2006. E-passports contain a chip which stores the passport holder's facial biometric. According to the then-Minister of State for Immigration Brandon Lewis no other biometric information is captured on British e-passports.[32]

All Non-EU migrants who come to the UK for longer than six months, extend their visas to longer than 6 months or who apply to settle in the UK under the UK's immigration rules are issued with a Biometric Residence Permit ("BRP"). This applies to all categories of UK visas such as family and work visas. The BRP will include the person's name, date and place of birth, fingerprints and photograph. Those applying for asylum in the UK must also provide their fingerprints and a photograph.

In response to a PQ on the use of biometrics in settled status applications, the Minister of State for the Home Office Baroness Williams of Trafford stated:

> Biometrics enrolled as part of an application to EU Settlement Scheme will be retained in accordance with the Immigration (Physical Data) Regulations 2006, as amended. In practice, this means that fingerprints will normally be retained for up to 10 years, unless the person has settled status or is considered to be a risk of high harm to the UK.
>
> All fingerprints are deleted from the Immigration and Asylum Biometric System when the person becomes a British citizen. Facial images may be retained until the person becomes a British citizen and obtains a British passport. Biometrics may only be retained as long as the Secretary of State considers it is necessary to retain them for use in connection with the exercise of a function by virtue of the Immigration Acts or a function in relation to nationality.[33]

The biometrics strategy recognises that ad hoc and parallel biometric capabilities have been developed by the Home Office for policing and immigration purposes which "can be inefficient and affect the delivery of services."[34] In response the Home Office proposes the Home Office Biometrics Program (HOB) to improve biometric services and processes across the department. This would entail a simple platform for the Home Office to more efficiently deal with the data from existing biometric processes:

> The effect of these changes will be to improve continuity, reduce operational costs, support future changes and increase confidence in the robustness of the techniques being used. Through a more consistent, centralised development, this will help increase confidence that legal standards and ethical implications have been taken into account as new uses are developed. This will include ensuring that services have in-built safeguards so that only necessary and proportionate access to biometric data is allowed, for specific roles and purposes. It will also support a more consistent approach to retention.[35]

[32] PQ 116960

[33] PQ HL 11784

[34] Home Office, Biometrics Strategy Better public services: Maintaining public trust, June 2018, para 13

[35] Ibid, para 15

1.4 Biometrics and data protection

The processing of personal data must comply with the General Data Protection Regulation (GDPR) and the *Data Protection Act 2018*.

A guide published by the Information Commissioner's Office (ICO) explains when personal data can be lawfully processed and the principles that apply.

There are tighter controls for processing special category data. The ICO guide includes further detail on these. Special category data includes biometric data and genetic data.[36]

Processing for law enforcement purposes

Part 3 of the 2018 Act applies to "competent authorities" who are processing personal data for law enforcement purposes. Competent authorities include:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

An ICO guide on law enforcement processing summarises the conditions allowing the processing of special category data. These include processing for judicial and statutory purposes and the administration of justice.

Competent authorities are required to demonstrate accountability through:

- Data protection impact assessments (DPIAs) – these are 'an assessment of the impact of the envisaged processing operations on the protection of personal data'. A DPIA must be carried out before processing personal data where this is likely to result in a high risk to the rights and freedoms of individuals;
- Data protection officers (DPOs) – these help to monitor internal compliance, inform and advise on data protection obligations, provide advice on DPIAs and act as a contact point for data subjects and the ICO;
- Data protection by design and by default – i.e. implementing technical and organisational measures, at the earliest stages of the design of processing operations, to safeguard privacy and data protection principles.

The Biometrics Strategy

Much of the Biometrics Strategy involves processing for law enforcement purposes. The Strategy acknowledges the need to avoid

[36] Special category data also includes data that reveals a person's: racial origin; ethnic origin; political opinions; religious beliefs; philosophical beliefs; trade union membership; health data; sex life; sexual orientation

risks and protect the privacy of the individual when using biometric technologies.[37] Chapter 3 sets out how the Government intends to maintain public trust including through:

- DPIAs prior to the use of a new biometric technology or a new application of an existing biometric technology, inviting scrutiny from an independent ethics panel, regulators and commissioners
- DPIAs for each element of the Home Office Biometrics Programme[38]

Further detail on DPIAs is given on pp15-6 of the Strategy.

The Strategy also notes that the introduction of DPOs "will have a positive impact on the use of this [biometric] sensitive personal data but there will be a need to maintain and develop specific standards for key sectors that use biometrics".[39]

[37] Home Office, Biometrics Strategy, June 2018, p4
[38] Ibid, p13
[39] Ibid, para 51

2. News and blogs

The Telegraph

Why we should all be worried about Britain's facial recognition experiment

2 February 2019

The Telegraph

Britain's data commissioner launches investigation into UK use of Facial recognition

3 December 2018

Financial Times (subs)

We must face up to the threat posed by biometrics

8 August 2018

New Statesman

The Home Office's biometrics strategy is not a strategy, say critics

2 July 2018

The Telegraph

Facial recognition to be ramped up across British borders

29 June 2018

Guardian

Police face legal action over use of facial recognition cameras

14 June 2018

Daily Mail

Police's controversial use of Big Brother-style facial recognition and biometric technologies to catch criminals is 'running ahead of the law'

6 June 2018

The Independent

Metropolitan Police's facial recognition technology 98% inaccurate, figures show

13 May 2018

3. Parliamentary Business

3.1 Lords debate

Security and Policing: Facial Recognition Technology

HL Deb 1 March 2018 vol 789

3.2 Parliamentary questions

Identification of Criminals: Biometrics

Asked by: Jo Stevens

To ask the Secretary of State for the Home Department, how many police forces in England and Wales were using facial recognition software as of January 2019.

Answering member: Mr Nick Hurd | Department: Home Office

Facial recognition software takes two main forms. The first compares an image of an unknown person (for example caught on CCTV committing a crime, reviewed after the event) against a database of facial images of people who have been arrested. All police forces use the Police National Database facial search facility.

The second form is live facial recognition (LFR), which compares images of passers-by taken from live cameras with images on a watch list (a database of suspects). The Metropolitan Police Service and South Wales Police are piloting LFR. The pilots are important to test this technology, which has the potential to improve public safety. Both forces have commissioned independent reviews of the pilots.

The Law Enforcement Facial Images and New Biometric Modalities Oversight and Advisory Board oversees the police use of LFR, the retention of custody images, and emerging new biometrics. The Board’s minutes are published on GOV.UK

HC Deb 4 Mar 2019 | PQ226692

Police: Biometrics

Asked by: Baroness Jones of Moulsecoomb

To ask Her Majesty's Government which provisions of the General Data Protection Regulations police forces rely on when processing photographs taken by the police using facial recognition technology.

Answering member: Baroness Williams of Trafford | Department: Home Office

The police process personal data for law enforcement purposes under Part 3 of the Data Protection Act 2018. ‘Law enforcement purposes’ is defined in the Act as processing 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.

HL Deb 26 Nov 2018 | PQ11384

Police: Biometrics

Asked by: Lord Scriven

To ask Her Majesty's Government what assessment they have made of the annual report of the Commissioner for the Retention and Use of Biometric Material, published in March; and whether they intend to bring forward legislation to govern the use of automated facial recognition by the police.

Answering member: Baroness Williams of Trafford | Department: Home Office

The Government published its response to the Biometrics Commissioner's Annual Report on 5 June on the gov.uk website.

On the issue of legislation on police use of automated facial recognition, I refer the noble Lord to the answer I gave to his question HL8083 on 4 June.

HL Deb 21 Jun 2018 | PQ8456

Police: Biometrics

Asked by: Lord Scriven

To ask Her Majesty's Government, further to the Written Answer by Baroness Williams of Trafford on 4 June (HL8083), how the Information Commissioner's Code of Practice relating to the police use of facial recognition technology is enforced.

Answering member: Baroness Williams of Trafford | Department: Home Office

The Information Commissioner's Office (ICO) issues guidance under Data Protection Legislation. It is for the ICO to determine how to take enforcement action under this legislation.

HL Deb 18 Jun 2018 | PQ8376

Police: Biometrics

Asked by: Lord Scriven

To ask Her Majesty's Government what plans they have to introduce legislation on the use of facial recognition technology by police forces.

Answering member: Baroness Williams of Trafford | Department: Home Office

Facial recognition software is a new and potentially valuable law enforcement tool in reducing crime and protecting the public. Police forces are obliged, under the Protection of Freedoms Act, to have regard to the Surveillance Camera Code of Practice which requires the use of facial recognition systems to be clearly justified and proportionate in meeting its stated purpose.

Similarly, the Information Commissioner's Office has issued a Code of Practice, which explains how data protection legislation applies to the use of surveillance cameras and promotes best practice. The College of Policing's Authorised Professional Practice governs the retention of facial images. The Government also plans to improve independent oversight and governance of police use of the technology.

HL Deb 04 Jun 2018 | PQ8083

Police: Biometrics

Asked by: Paul Girvan

To ask the Secretary of State for the Home Department, if he will take steps to ensure that the facial recognition software that law enforcement bodies use is accurate.

Answering member: Mr Nick Hurd | Department: Home Office

Facial recognition systems can be used to compare people in public spaces to images on a pre-determined list and provide suggested matches to a human operator. The rate of suggested matching will depend on the system, the images and the circumstances of the deployment. They will produce false positive matches which it would be for the operator to consider including any follow up procedure.

The decision to deploy such systems is an operational one for police forces but they must comply with Data Protection Legislation and show regard to the Surveillance Camera Code of Practice, the Information Commissioner's Code of Practice and other relevant policies and legislation.

HC Deb 24 May 2018 | PQ145395

Police: Biometrics

Asked by: Louise Haigh

To ask the Secretary of State for the Home Department, pursuant to the Answer of the 30 April 2018 to Question 138075, on Biometrics, how the Government plans to improve the independent oversight and the governance of police use of automated facial recognition software.

Answering member: Mr Nick Hurd | Department: Home Office

The Government will create a Board including the three relevant regulators (the Biometrics Commissioner, Surveillance Camera Commissioner and Information Commissioner) and police representatives. It will facilitate open dialogue between regulators and police forces that are considering piloting such technology.

The Board will also consider all aspects of public trust in the police’s use of this technology, bringing together ethical and privacy considerations.

HC Deb 03 May 2018 | PQ139541

4. Further reading

Home Office, Biometrics Strategy: Better public services, Maintaining public trust, June 2018

Government Office for Science, Biometrics, a guide, 2018

Commissioner for the retention and use of biometric material, Annual Report 2017, March 2018

Science and Technology Committee, Biometrics strategy and forensic science, 25 May 2018, HC800 2017-19

Science and Technology Committee, Biometrics strategy and forensic services: Government’s Response to the Committee’s Fifth Report, 15 October 2018, HC1613 2017-19

Home Office and Biometrics Commissioner

Biometrics Commissioner annual report for 2018

23 April 2019

Big Brother Watch

Big Brother Watch launches legal challenge to Government and Met Police on “dangerously authoritarian” facial recognition cameras

14 June 2018

Elizabeth Denham, Information Commissioner

Facial recognition technology and law enforcement

14 May 2018

Biometric Technologies, Commons Library POST briefing, 29 June 2018

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer

This information is provided to Members of Parliament in support of their parliamentary duties. It is a general briefing only and should not be relied on as a substitute for specific advice. The House of Commons or the author(s) shall not be liable for any errors or omissions, or for any loss or damage of any kind arising from its use, and may remove, vary or amend any information at any time without prior notice.

DEBATE PACK
CDP 2019/0099
30 April 2019