BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch Briefing for Short Debate on the use of facial recognition technology in security and policing in the House of Lords, 1st March 2018

February 2018

Short debate: Thursday 1st March, Main Chamber, House of Lords

Baroness Jones of Moulsecoomb to ask Her Majesty's Government what proposals they have for the use of facial recognition technology in security and policing.

Speakers' List:

Lord Evans of Weardale

Lord Kennedy of Southwark

Lord Paddick

Lord Scriven

Contents

Summary

We urge Parliamentarians to

- call on the Home Office to **immediately stop police forces using automated facial recognition software with surveillance cameras**, and
- call on the Home Office to **automatically remove the thousands of images of unconvicted individuals from the custody image database.**

Introduction

In this briefing, we focus on police forces' use of automated facial recognition technology and seek to inform parliamentarians of the significant risks it poses to civil liberties and the rule of law in the UK.

- We seek to draw your attention to the facts: that there is **no law, no oversight, and no policy** regulating the police's use of automated facial recognition.

- We also explain why automated facial recognition has proven to be an **ineffective policing tool** producing high numbers of 'false positive' matches.

- Furthermore, research has found that many automated facial recognition algorithms have **discriminatory effect,** disproportionately misidentifying black and female faces.

- Finally, we discuss the **impact of automated facial recognition on human rights** in the UK and question whether such biometric checkpoints are, or could ever be, compatible with the rights framework.

Secondly, we raise the issue that the custody image database is **oversized and is highly likely to retain images unlawfully**. The antiquated database of 21 million photos stores images of innocent people who neither received a conviction nor are of any policing interest. The storage of such photos was ruled unlawful in 2012 by the High Court in *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department.* However, it is this database with which facial recognition technology is used by police.

Therefore, it is clear that that:

- The custody image database, which provides the basis for both facial matching and automated facial recognition, unnecessarily contains a significant proportion of photos of innocent people under what is likely to be an unlawful retention policy;
- There is no legal basis for the police's use of automated facial recognition with public surveillance cameras, and given the significant interference of this technology with fundamental rights, its use should be immediately ceased.

Finally, we consider the use of facial recognition technology by UK security and intelligence agencies.

About facial recognition

Facial recognition technology measures and matches unique facial characteristics for the purposes of biometric surveillance or identification.

There are two major strands within facial biometrics

- **Facial Matching**: this is the matching of an isolated, still image of an individual against a database. This is used at borders with biometric passports and by police to match images of suspects against images on the Police National Database.

- **Automated Facial Recognition**: this is a new technology which matches faces captured by a live camera feed against a database (either a custody image database, or a smaller subset of the database) in real time.

> *Facial recognition technology aims to identify individuals or authenticate individuals by comparing their faces against a database of known faces and looking for a match.*
>
> *The process can be broken down into three very general steps.*
>
> ***First, the computer must find the face in the image.***
>
> ***It then creates a numeric representation of the face based on the relevant position, size and shape of facial features.***
>
> ***Finally, this numeric map of the face in the image is compared to a database of images of identifies faces.***
>
> \- *South Wales Police*

In the UK, South Wales Police is leading the deployment of automated facial recognition and benefits from £2m funding from the Home Office to do so.[1] Since May 2017, South Wales has been using this surveillance technology prolifically: at football games, rugby matches, boxing events, concerts and shopping centres.

The Metropolitan Police has also been deploying automated facial recognition since 2016. Leicestershire Police trialled the technology at Download Festival in 2015.

[1] https://pcclivewww.blob.core.windows.net/wordpress-uploads/2016-12-28-Final-Medium-Term-Financial-Strategy.pdf

The use of facial recognition technology in policing

No law

1. There is no clear legal basis for UK police forces' use of automated facial recognition technology.

2. When Layla Moran MP posed a written question to the Home Office about current legislation regulating "*the use of CCTV cameras with facial recognition and biometric tracking capabilities*", Nick Hurd MP (Minister for Policing, responding for the Home Office) answered: *"There is no legislation regulating the use of CCTV cameras with facial recognition"*.[2]

> ***"There is no legislation regulating the use of CCTV cameras with facial recognition".***
>
> **- Nick Hurd, Minister for Policing – September 2017**

3. The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras in England and Wales. As a result the Surveillance Camera Code of Practice was issued by the Secretary of State in 2013 under section 30 of the Act. There is no reference to facial recognition in the Protection of Freedoms Act, although it provides the statutory basis for public space surveillance cameras.

4. Neither House of Parliament has ever considered or scrutinised automated facial recognition technology. To do so after its deployment is unacceptable – particularly given the technology's significant and unique impact on rights.

5. The Surveillance Camera Commissioner has himself raised the issue of the lack of a clear statutory footing for facial recognition.[3]

6. There are but three passing references to facial recognition in the Surveillance Camera Code of Practice. This paucity of guidance cannot be considered a suitable regulatory framework for facial recognition.

[2] Written parliamentary question answered by Mr Nick Hurd MP on 12 September 2017.

[3] For example, in *A National Surveillance Camera Strategy for England and Wales* – Surveillance Camera Commissioner, March 2017, para. 35, p.12

No oversight

7. There is no independent oversight provision for automated facial recognition. Police forces using the technology have claimed that they consult the Information Commissioner's Office and Surveillance Camera Commissioner, and sometimes the Biometrics Commissioner.

8. However, the oversight of facial recognition is not formally within the remit of the any of the above. The Surveillance Camera Commissioner noted: "*Clarity regarding regulatory responsibility is an emerging issue, for example in automatic facial recognition use by police – which regulator has responsibility – the Biometric Commissioner, the Information Commissioner or Surveillance Camera Commissioner."*[4]

9. The Science and Technology Committee recommended that such oversight fall within the Biometrics Commissioner's remit in 2015, as did the (then) Commissioner. This may be preferable to the oversight falling to the Surveillance Camera Commissioner as the use of the technology could be considered in multiple environments, not restricted to overt public surveillance cameras. However, Government has not acted on the suggestion and facial recognition remains without oversight, beyond the remit of the Commissioner's role.

What databases can be matched against, for what purposes the technology can and cannot be used, which images are captured and stored, who can access those images, how long they are stored - are all questions without answers.

No policy

10. The Government said the Home Office would publish a 'Forensics and Biometrics Strategy' by 2013. This didn't happen. The Home Office has missed its own deadline to produce a strategy for the use of facial recognition by over four years and running - despite finding the time and millions of pounds to fund new deployments of the technology. After yearly promises and missed deadlines, the Home Office recently promised to publish the Biometrics Strategy in June 2018.

11. There is no known policy or guidance regulating the use of automated facial recognition technology. What databases can be matched against, which images are captured and

[4] *Review of the impact and operation of the Surveillance Camera Code of Practice* –Surveillance Camera Commissioner, Feb 2016, p.15

stored, who can access those images, how long they are stored - are all questions without answers.

12. Neither is there any policy limiting the purposes for which individuals can be identified by the technology. At Remembrance Sunday In November 2017, the Metropolitan Police used automated facial recognition to match against a dataset of 'fixated individuals' – people who are known to frequently contact public figures and are highly likely to suffer mental health issues, but not people who were known to be engaging in criminal activity or who were wanted for arrest. This non-criminal application of facial recognition technology resulted in a so-called 'fixated individual' being identified and subsequently dealt with by police.

An ineffective tool

13. Automated facial recognition is currently an inaccurate and ineffective tool that has a high rate of misidentifications. Big Brother Watch is seeking the formal provision of relevant statistics relating to police forces' deployments of the technology. However, the officers operating automated facial recognition for the Metropolitan Police told Big Brother Watch that at their Notting Hill Carnival deployment in 2017, they had one positive match and 'around 35' false-positive matches. They also reported that this led to police pursuing 'around five' innocent people to request they authenticate their identity. On the basis of this data, only 2.8% of 'matches' generated by automated facial recognition technology were accurate – over 97% of alerts were erroneous matches of innocent people.

14. However, Big Brother Watch observed the Metropolitan Police's use of the technology at Notting Hill Carnival 2017 for a short 5-10 minute period. During that brief time, we observed two false-positive matches, both matching innocent women walking past with men on the database. If erroneous 'matches' are being generated at the rate we observed, one would expect to see around 100 false-positive matches a day. It is possible that the figures we were given were conservative estimates.

> ***On the basis of this data, only 2.8% of 'matches' generated by automated facial recognition technology were accurate – over 97% of alerts were erroneous matches of innocent people.***

15. The Metropolitan Police's 'positive match' at Notting Hill Carnival 2017 was also a failure and waste of police time. The data against which police were matching the CCTV feed was stale – the individual who was flagged and apprehended was no longer wanted for arrest.

Discrimination

16. Several studies have found that commercial facial recognition algorithms, including those used by law enforcement, have demographic accuracy biases – that is, they are better at recognising some groups' faces than others. In March 2017, the US Government Accountability Office found that facial recognition algorithms used by the FBI are inaccurate almost 15% of the time and are more likely to misidentify female and black people. This could be due to bias coded into the software by programmers, albeit unintentionally, and/or due to an under-representation of black people and women in the training datasets used to develop the software.

Research has found that some facial recognition algorithms are more likely to misidentify black faces

17. In the context of law enforcement, biased facial recognition algorithms risk leading to disproportionate interference with the groups concerned – whether through police stops and requests to show proof of identity, or through the police's storage of matched images. However, the commercial facial recognition software used by South Wales Police and the Metropolitan Police has not been tested for demographic accuracy biases. In our engagement with Metropolitan Police, we have urged the force to seek such testing. We were extremely disappointed to encounter resistance from the police to the idea that such testing is important or necessary,

18. Many organisations are concerned by this technology, and the risk of it carrying invisible, unaccountable demographic biases. Before the Metropolitan Police used automated facial recognition for the second time at Notting Hill Carnival in 2017, Big Brother Watch, Police Action Lawyers Group, the Race Equality Foundation, and 10 other rights and race equality groups signed a joint letter to the Force raising our concerns and calling for a halt to the deployment.

Human Rights Act

19. Even if automated facial recognition technology was proven to be accurate, both in terms of demographic accuracy and the general rate at which matches are accurate, outstanding questions remain as to whether it is appropriate in a democratic society; whether it risks impacting civil liberties; and specifically, whether it is compatible with the Human Rights Act.

20. In Big Brother Watch's view, the use of automated facial recognition with public surveillance cameras presents a serious interference with fundamental rights to a private life and freedom of expression. This border-style security tool puts biometric identity checkpoints onto our streets. It is plainly disproportionate to deploy a technology by which the face of every passer-by is analysed, mapped and their identity checked.

Custody images and facial recognition

21. Section 64A of the Police and Criminal Evidence Act 1984 (PACE) provides police with the power to take facial photographs (custody images) of anyone who is detained following arrest. Forces can upload custody images from their local IT systems onto the Police National Database ('PND'), which has been in place since 2010. Police started using biometric facial recognition with the PND on 28th March 2014. As of February 2018, there were 21 million custody images on PND, of which 12.5 million are biometric and searchable.[5]

There are 21 million custody images on Police National Database, of which 12.5 million are biometric and searchable.

22. In 2015, the parliamentary Science and Technology Committee reported:

"In the absence of a biometrics strategy, there has been a worrying lack of Government oversight and regulation of aspects of this (biometrics) field.

We were particularly concerned to hear that the police are uploading photographs taken in custody, including images of people not subsequently charged with, or convicted of, a crime, to the Police National Database and applying facial recognition software.

[5] http://www.dailymail.co.uk/wires/pa/article-5379353/Custody-image-deletion-request-figures-revealed.html

Although the High Court ruled in 2012 that existing policy concerning the retention of custody photographs by the police was "unlawful", this gap in the legislation has persisted."[6]

23. The High Court found in *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012],* cited above, that the policy to retain custody images of individuals who were not convicted was unlawful. However, have the police continued to store such custody images. In February 2017, following a review, the Government gave unconvicted individuals the option to write a letter to the relevant police force to request deletion of their image from the custody image database. This obstructive policy shirks responsibility from the Home Office, which clearly needs to automatically delete the thousands of images stored of innocent people.

24. The new policy was exposed as a failure by a recent Press Association investigation which found that only 67 applications for deletion had been made, of which only 34 were successful. Norman Lamb MP, Chair of the Science and Technology Committee, publicly commented on his concerns that the Home Office's retention and deletion policy is likely to be unlawful.[7]

25. In his 2016/17 Annual Report, the SCC commented:

"[The Custody Images Review 2017] directly relates to the use of automatic facial recognition systems because ***the police will seek to utilise this database to build the systems for cross checking live feeds from surveillance cameras*** *against this database."*[8]

Of course, we are now witnessing police forces do exactly that, using subsets of the custody image database to match against live CCTV feeds with automated facial recognition software.

The use of facial images by the police has gone far beyond using them for custody purposes

- The Biometrics Commissioner, September 2017

[6] https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf
[7] Arrangements for storing millions of `custody images´ may be unlawful, MP says – 14 February 2018 http://www.dailymail.co.uk/wires/pa/article-5389875/Arrangements-storing-millions-custody-images-unlawful-MP-says.html
[8] The Surveillance Camera Commissioner's Annual Report 2016/17

26. In his 2016 Annual Report, the Biometrics Commissioner commented:

> "***The use of facial images by the police has gone far beyond using them for custody purposes*** *(...) (U)nlike DNA or fingerprints, facial images can easily be taken and stored* ***without the subject's knowledge*** *and facial images of about 90% of the adult population already exist in passports or driving licences."*[9]

Clearly, the potential for the growth of a gargantuan facial recognition system is a real risk, and arguably would be the natural destination for this technology, if we accept its use now.

[9] Annual Report – Commissioner for the Retention and Use of Biometric Material, Paul Wiles, September 2017, para. 301-5

The use of facial recognition technology in security

27. Little is known about the security and intelligence agencies' use of facial recognition technology, whether for matching still images or live surveillance camera feeds.

28. However, of the most shocking revelations to be documented by NSA whistleblower Edward Snowden was a GCHQ program called Optic Nerve, in which millions of innocent people were spied on through their webcams to secretly take photos and experiment with facial recognition. Under the program, from 2008, the Agency intercepted webcam chats in bulk, without suspicion, and covertly took screenshots of over 1.8m callers in 6 months alone. The images were searched to monitor current targets and discover new targets. [10]

> ***In 2008, GCHQ spied on innocent people through their webcams, covertly taking millions of images and running facial recognition technology to search for targets as well as to "discover new targets".***

29. Ten years ago, GCHQ was indiscriminately spying on millions of innocent people through their webcams and checking their identities as they enjoyed what they thought were private conversations in their own homes. Big Brother Watch and other NGOs are currently challenging s.8.4 of the Regulation of Investigatory Powers Act (RIPA), from which the security and intelligence agencies claimed to draw the power to conduct mass interception, on the basis that it clearly constitutes a disproportionate interference with the right to private life under Article 8 of the European Convention on Human Rights. However, disturbingly, the power to conduct bulk interception is explicitly provided for in the Investigatory Powers Act (IPA) 2016, now subject to judicial review by Liberty. The IPA also gives intelligence agencies a broad power to collect and process 'bulk personal datasets' – under which datasets like the passport database and DVLA database, containing over 90% of the population's facial images, can be used for monitoring. With advances in technology in the past decade, and the advent of blank cheque surveillance laws, it is difficult to imagine how extensively the intelligence agencies may be using facial recognition technology today.

[10] Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ – James Ball and Spencer Ackerman, 28 Feb 2014, The Guardian: https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation. We hold to account those who fail to respect our privacy, and campaign to give individuals more control over their personal data. We produce unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Contact

Silkie Carlo

Director

Direct line: 020 7340 6042

Email: silkie.carlo@bigbrotherwatch.org.uk