LIBERTY

LIBERTY'S BRIEFING ON POLICE USE OF LIVE FACIAL RECOGNITION TECHNOLOGY

November 2019

ABOUT LIBERTY

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at libertyhumanrights.org.uk/policy.

CONTACT

HANNAH COUCHMAN

Policy and Campaigns Officer

020 7378 5255 | hannahc@libertyhumanrights.org.uk

GRACIE BRADLEY

Policy and Campaigns Manager

020 7378 3654 | gracieb@libertyhumanrights.org.uk

CONTENTS

INTRODUCTION

1. Facial recognition is currently being trialled by South Wales Police (SWP), and the Metropolitan Police Service (the Met) is due to make a decision on wider roll-out in the coming months following the completion of just ten trial deployments. A recent independent review of the Metropolitan Police's trial of facial recognition[1] criticised the force for failing to consider the impact of this technology on human rights and for relying on an inadequate legal basis.[2]

2. Meanwhile, private company use – often in partnership with local police forces – is expanding. There is no law regulating its use, and there has been no public or parliamentary discussion of the highly damaging impact of this technology on human rights.

3. The use of facial recognition by both the Met and SWP is subject to legal action from civil liberties organisations. Liberty is currently seeking permission to appeal the High Court's recent judgment[3] in relation to Ed Bridge's case[4] which challenged the use of facial recognition by SWP. Big Brother Watch will pursue litigation against the Met if they choose to roll out operational use facial recognition technology.[5]

4. Police use of facial recognition in public spaces is an enormous infringement of privacy for everyone who passes by the camera. In addition to being discriminatory and inaccurate, it is a mass surveillance tool. Being able to choose when and how to disclose one's identity, and to whom, is at the heart of a person's dignity and autonomy. Furthermore, identification determines how the State interacts with people, and in some cases, whether they can access their rights. The use of facial recognition therefore represents a huge shift in the relationship between the individual and the State, and for our right to remain anonymous more broadly. The human rights impact of its indiscriminate and non-consensual nature means that it should have no place on our streets.

HOW FACIAL RECOGNITION WORKS

5. Live facial recognition[6] works by matching images of people walking past facial recognition cameras against images on a "watch list". The cameras scan the distinct facial points of each passer-by and create a uniquely identifiable biometric map in the form of a numerical code, which is then matched against corresponding codes from images of people on police watch lists. This deeply intrusive

[1] Fussey et al (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* , University of Essex, Available at: https://www.hrbdt.ac.uk/publications/?wpdmc=facial-recognition-download
[2] See paragraphs 22-24 below
[3] Liberty (2019), *Liberty fights for facial recognition ban following court ruling* [Press Release], 4 September 2019, Available at: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/liberty-fights-facial-recognition-ban-following-court-ruling The Court found that facial recognition interferes with the privacy rights of everyone scanned, but that use is currently lawful.
[4] Liberty (2018), *Cardiff man gets go-ahead to bring first UK legal challenge to police use of facial recognition technology on the streets* [Press Release], 2 July 2018, Available at: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/cardiff-man-gets-go-ahead-bring-first-uk-legal-challenge-police
[5] Big Brother Watch (2018), *Big Brother Watch Begins Landmark Legal Challenge to Police Use of Facial Recognition Surveillance* [Press Release], 25 July 2018, Available at: https://bigbrotherwatch.org.uk/all-media/big-brother-watch-begins-landmark-legal-challenge-to-police-use-of-facial-recognition-surveillance
[6] Police forces may refer to live facial recognition as "AFR Locate", to distinguish it from non-live facial recognition programs used to match still photographs to a watch list ("AFR Identify"). All references to facial recognition in this briefing refer to the use of facial recognition in live settings.

technology is being deployed at sporting events, concerts and festivals, in city centres, on busy shopping streets, as part of everyday police operations – and even at protests.[7]

6. Watch lists are curated by the police and shrouded in secrecy. There is no specific regulation as to who can be placed on a watch list, or what sources can be used. Documents produced in the course of the litigation against SWP confirmed that anyone could be included on a watch list – including people who are not wanted by the police or the courts.[8] The Met used facial recognition to monitor people at Remembrance Sunday in 2017, and aimed to exclude people from a public remembrance event on the basis that they had a mental health condition.[9] Watch lists may also include images obtained from social media.[10] The Information Commissioner has stated that *"watchlists comprising large numbers of individuals where there is no reasonable expectation that they will be in the vicinity of the LFR deployment are...likely to lead to concerns about strict necessity and proportionality and about compliance with data protection principles".* [11]

7. Unlike other biometric systems utilised by law enforcement, such as fingerprinting, facial recognition can be used for passive and general surveillance and does not require the knowledge, consent or active participation of the people being monitored.

RISKS TO HUMAN RIGHTS

THE RISK TO OUR PRIVACY

8. The Human Rights Act 1998 ("HRA") gives effect in domestic law to the European Convention on Human Rights (ECHR). Article 8 ECHR requires that any interference with the right to a private life is in accordance with law and is both a necessary and proportionate means for achieving a legitimate aim. In Liberty's view, the use of facial recognition in public spaces fails to meet these thresholds. To the extent that it involves indiscriminately scanning, mapping and checking the identity of every person within the camera's range – using their deeply sensitive biometric data – it is an enormous interference with the right to privacy.

9. While facial recognition has a significant privacy impact when it works, it also has a significant privacy impact when it does not. A "false match" occurs where someone is stopped following a facial recognition match but is not, in fact, the person included on the watch list. In the event of a false match, a person attempting to go about their everyday life is subject to an invasive stop and may be required to show

[7] South Wales Police list their deployments of facial recognition online (see: http://afr.south-wales.police.uk/#deployments). The Met have deployed facial recognition on ten occasions Notting Hill Carnival in 2016 and 2017, Remembrance Day 2017, Port of Hull docks (in partnership with Humberside Police) in 2018, Stratford transport hub for two days in June and July 2018, Central London in December 2018 and Romford for two days in January and February 2019. Leicestershire police deployed facial recognition at Download Music Festival in 2015 (see: https://www.independent.co.uk/news/uk/crime/download-festival-facial-recognition-technology-used-at-event-could-be-coming-to-festivals-10316922.html).
[8] Manthorpe (2019), *Police facial recognition could target 'literally anybody', senior MP says*, Sky News, 26 July 2019, Available at: https://news.sky.com/story/police-facial-recognition-could-target-literally-anybody-senior-mp-says-11770696
[9] Townsend (2017), *Police to use facial-recognition cameras at Cenotaph service,* The Guardian, 12 November 2017, Available at: https://www.theguardian.com/technology/2017/nov/12/metropolitan-police-to-use-facial-recognition-technology-remembrance-sunday-cenotaph
[10] Davies et al (2018), *An Evaluation Of South Wales Police's Use Of Automated Facial Recognition*, Universities' Police Science Institute, University of Cardiff, Available at: http://www.statewatch.org/news/2018/nov/uk-south-wales-police-facial-recognition-cardiff-uni-eval-11-18.pdf
[11] The Office of the Information Commissioner (2019), *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places,* Reference: 2019/01, Available at: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

identification, account for themselves and even be searched under other police powers. Liberty has observed a distinct lack of human oversight over live matches[12] and has significant concerns about decisions of this nature being influenced by complex and impenetrable technology.

10. The privacy concerns examined throughout this briefing cannot be addressed simply by requiring the police to delete images captured of passers-by, or by improving the accuracy of the technology. Inaccurate facial recognition results in a high rate of false stops and corresponding rights infringements. However, accurate facial recognition will simply ensure that everyone's privacy rights are equally infringed.

THE RISK TO OUR FREEDOM OF EXPRESSION AND ASSOCIATION

11. The ECHR requires that any interference with the Article 10 right to free expression, or Article 11 right to free association, is in accordance with law, and both necessary and proportionate. The use of facial recognition technology can be highly intimidating. If we know our faces are being scanned by police and that we are being monitored when using public spaces, we are more likely to change our behaviour.[13] Those changes in behaviour may relate to where we go and who we choose to associate with. For a whole host of reasons linked to a desire to retain our anonymity and to keep our activities and political views private, we may decide not to attend public meetings, to avoid our local high street, or change who we spend time with in public spaces. For example, Liberty has worked with protesters who expressed how intimidating they found the presence of facial recognition at demonstrations, and who said that they would be reluctant to attend a future protest where it was in use.

12. Even where images or biometric data are not retained following a deployment of facial recognition, this technology could still be used to identify that a known person was at an event and this could be recorded through traditional methods. The UK has a shameful history of subjecting political activists to invasive state surveillance. The European Court of Human Rights recently held that the UK had violated the right to privacy of Mr John Catt, a peace movement activist who – despite having never being convicted of any offence – had his name and other personal data included in a police database and was subject to intrusive surveillance.[14]

13. If facial recognition interacts with other surveillance technologies, people are increasingly likely to feel that they have no choice but to avoid expressing religious or dissenting political views in public, and may consequently avoid attending demonstrations, political meetings or places of worship. As a society, this will undermine our ability to express ideas and opinions, communicate with others and engage in democratic processes, as people increasingly choose not to pay the price of handing over their sensitive biometric data in order to do so. The Conservative MP Eleanor Laing has recognised that people who are

[12] Liberty observers witnessed the stop of a man following a false match at a Met deployment. There was no observable human verification process to assess the match before the man was stopped. See Couchman (2018), *"Not A Fool-Proof System": Facial Recognition In Action* [Blog], 29 June 2018, Available at: https://www.libertyhumanrights.org.uk/news/blog/%E2%80%9Cnot-fool-proof-system%E2%80%9D-facial-recognition-action

[13] Studies have shown that people were less inclined to attend mosques they thought were under government surveillance. Business owners muted political discussion by turning off Al-Jazeera in their stores, and activists self-censored their comments on Facebook. See: Shamas et al (2103), *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Muslim American Civil Liberties Coalition (MACLC), and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, Available at: http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[14] *Catt v United Kingdom* 43514/15, [2019] ECHR 76

"*going about their business and not breaking the law in any way might nevertheless fear for their privacy, because they do not intend their whereabouts at any particular point to be a matter for public record*".[15]

THE RISK TO OUR FREEDOM FROM DISCRIMINATION

14. Article 14 ECHR ensures that no one is denied their rights because of their gender, age, race, religion or beliefs, sexual orientation, disability or any other characteristic. Police use of facial recognition gives rise to two distinct discrimination issues: bias inherent in the technology itself and the use of the technology in a discriminatory way.

15. **Discriminatory use:** Liberty has raised concerns regarding the racial and socio-economic dimensions of police trial deployments thus far. For example, the Met has deployed facial recognition at Notting Hill Carnival for two years running, a festival celebrating West Indian culture in the UK, as well as twice in the London Borough of Newham. Newham is one of the UK's most ethnically diverse places and the white British population stands at 16.7%, the lowest in the UK. The disproportionate use of this technology in communities against which it underperforms (according to its proponent's standards) is deeply concerning.

16. The Office of the Information Commissioner also noted to the Science and Technology Committee that *"The Committee's view was that facial recognition technology should not generally be deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved. The Commissioner is concerned that this has not been fully addressed and it is not yet clear how the 'oversight board' will address these issues."*[16]

17. **Inherent bias:** Studies have shown facial recognition technology disproportionately misidentifies women and BAME people[17] – meaning that people from these groups are more likely to be wrongly stopped and questioned by police, and to have their images retained as the result of a false match. The same conclusion was reached in a study conducted by the FBI.[18] While the causes of discrimination within algorithms can vary, in this case it is likely to stem from the fact that, when an algorithm is trained to recognise human faces using training data sets, it is exposed to a disproportionate number of white, male faces compared to those from other groups.

18. However, Liberty notes that improving the accuracy of this technology only serves to increase the pervasiveness of the rights infringements associated with facial recognition. As Dr Julia Powles points out, *"even apparent success in tackling bias can have perverse consequences. Take the example of a facial recognition system that works poorly on women of color because of the group's*

[15] HC Debate, 19 March 2009, column 304, Available at: https://publications.parliament.uk/pa/cm200809/cmhansrd/cm090319/halltext/90319h0001.htm#09031961000280
[16] Written evidence submitted by Steve Wood, Deputy Commissioner for Policy, Information Commissioner's Office (WBC0008), The work of the biometrics commissioner and the forensic science regulator, March 2019, Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.html
[17] Buolamwini et al (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 2018 Conference on Fairness, Accountability, and Transparency
[18] Klare et al (2012), *Face Recognition Performance: Role of Demographic Information*, IEEE Transactions on Information Forensics and Security, Available at: https://ieeexplore.ieee.org/document/6327355.

underrepresentation both in the training data and among system designers. Alleviating this problem by seeking to "equalize" representation merely co-opts designers in perfecting vast instruments of surveillance and classification."[19]

THE FUTURE OF MASS SURVEILLANCE

19. The ubiquity of surveillance cameras, which can be retrofitted with facial recognition software and fed into police databases, means that there is already an apparatus in place for large-scale intrusive surveillance, which could easily be augmented by the widespread adoption of facial recognition technology. Use of facial recognition technology in the private sector could also result in the build-up of large repositories of photographs or the associated biometric data, which could be requested by police for law enforcement purposes. A 2015 survey of 150 retail executives by the IT services firm Computer Services Corporation suggested that a quarter of all British shops use facial recognition – and it is highly likely that this number has since increased.[20]

20. There have also been concerning developments in terms of private company use of police data. In October 2018, it was revealed that the Trafford Centre in Manchester had scanned the faces of every visitor for a six-month period, using watch lists provided by Greater Manchester Police[21] - approximately 15 million people.[22] Recent reports also revealed that live facial recognition was being used at the privately-owned but publicly-accessible site around King's Cross station, and that both the Met and British Transport Police had provided images for their use – despite originally denying doing so.[23] The Surveillance Camera Commissioner has noted the dangers of private companies utilising police data in this way.[24]

21. The risks presented by continued expansion of facial recognition include the use of this technology through the pre-existing CCTV network and body-worn video, enabling passive, real-time monitoring of us all – entirely without suspicion and without our knowledge or consent. Despite the fact that SWP's use of facial recognition is still in a "pilot" stage[25], SWP have made known their plans to make this technology "portable" through digital Samsung Galaxy devices,[26] as well as recognising the potential for it to be used in conjunction with police body worn video and CCTV.[27]

---

[19] Powles (2018), *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*, Medium, 7 December 2018, Available at: https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

[20] CSC technology (now DXCTechnology) (2015), *Next Generation In-store Technology: Where do Shoppers and Retailers Stand*, Available at: https://turtl.dxc.technology/story/55ee93d8bbfd077f2d4e22ee

[21] Robson (2018), *Greater Manchester Police monitored every visitor to Trafford Centre for SIX MONTHS using controversial technology until they were told to stop,* Manchester Evening News, 14 October 2018, Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-trafford-centre-camera-monitored-15278943

[22] Robson and Koncienzcy (2018), *How to find out if you were one of the 15 MILLION caught in a secret surveillance pilot,* Liverpool Echo, 15 October 2018, Available at: https://www.liverpoolecho.co.uk/news/liverpool-news/how-find-out-you-were-15284099

[23] BBC (2019), *Met Police gave images for King's Cross facial recognition,* 6 September 2019, Available at: https://www.bbc.co.uk/news/technology-49586582

[24] Porter (2018), *Working together on automatic facial recognition* [Blog], 10 October 2018, Available at: https://videosurveillance.blog.gov.uk/2018/10/10/working-together-on-automatic-facial-recognition/.

[25] SWP have not provided an end date for their "pilot" of facial recognition

[26] Police Inspector Scott Lloyd, South Wales Police Automated Facial Recognition Event, 4 February 2019, South Wales Police Headquarters, Bridgend, Wales.

[27] Ibid

NO LEGAL BASIS

22. In addition to the significant rights impacts of facial recognition technology, there is no law which gives the police the power to use facial recognition, and no Home Office policy covering its use. The Met have presented a tenuous legal basis relying on a combination of pre-existing legislation including the Police and Criminal Evidence Act 1984, the HRA, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Data Protection Act 2018 (DPA).[28] SWP has confirmed a similar approach[29] – despite the fact that these sources do not in any way provide a legal mandate for the use of this technology.

23. While the Protection of Freedoms Act 2012 and Police and Criminal Evidence Act 1984 contain provisions relating to police use of biometric data, these provisions do not extend to cover facial biometrics. The DPA specifically states that *"[t]he processing of personal data for any of the law enforcement purposes is only if and to the extent that it is based on law"*[30] – clarifying unequivocally that this legislation does not provide a legal basis for the use of facial recognition by law enforcement. Similarly, the HRA provides no such basis and specifically requires that any restriction on rights, where permissible, must be prescribed by law.

24. However, Liberty's view is that even if there were sufficient law regulating the use of this technology, it would still pose an unacceptable threat to human rights.

NO OVERSIGHT

25. It is not clear who provides oversight of the use of facial recognition, and Commissioners themselves have highlighted their confusion around responsibilities in this area.[31] The Home Office's Biometrics Strategy, which was delayed by over four years, has been widely criticised as failing to address this and other key issues. Norman Lamb, chairman of Parliament's Commons Science and Technology Select Committee, stated that it *"simply does not do justice to the critical issues involved".*[32] The Biometrics Commissioner described it as *"short sighted at best"*[33] and a *"disappointing document"*.[34]

26. The Biometrics Commissioner has recently stated that *"things like [facial recognition] systems are potentially going to affect the lives of every citizen – because this is mass surveillance through facial imaging…It seems to me very much in the public interest that that decision should be taken in a public way. And I would have thought the obvious body to do that was…Parliament",* adding that *"this would not be a sensible time to start routinely operationally deploying"*.[35]

[28] Met Police, *Live Facial Recognition trial* [Webpage], Available at: https://www.met.police.uk/live-facial-recognition-trial/
[29] Police Inspector Scott Lloyd, South Wales Police Automated Facial Recognition Event, 4 February 2019, South Wales Police Headquarters, Bridgend, Wales
[30] Section 35(2) DPA, Available here: https://www.legislation.gov.uk/ukpga/2018/12/section/35
[31] Surveillance Camera Commissioner (2016), *Review of the impact and operation of the Surveillance Camera Code of Practice*, Available at: https://www.gov.uk/government/publications/review-of-the-surveillance-camera-code-of-practice
[32] Hill (20118), *UK.gov's long-awaited, lightweight biometrics strategy fails to impress*, The Register, Available at: https://www.theregister.co.uk/2018/06/29/uk_biometrics_strategy/
[33] Ibid
[34] Professor Paul Wiles, Commissioner for the Retention and Use of Biometric Material, Oral evidence session: The work of the biometrics commissioner and the forensic science regulator, Science and Technology Committee**,** Tuesday 19 March 2019. Written record not yet available, Parliament TV available at: https://parliamentlive.tv/Event/Index/f9d3913e-b5c2-41e6-8452-de80f49e85e9
[35] Ibid

CONCLUSION

27. It is clear from the current and potential future human rights impact of facial recognition that this technology has no place on our streets. There has been no proper parliamentary or public debate about the use of this mass surveillance technology, denying Parliament the opportunity to consider or indeed neutralise the threat that it poses. Louise Haigh MP, Shadow Minister for Policing, has noted that "*[facial recognition] has been trialled for three years running. I suggest that it is no longer a trial. …Neither House of Parliament has ever considered or scrutinised automated facial recognition technology. To do so after its deployment—after three years of so-called trialling by the Metropolitan police—is unacceptable, particularly given the technology's significant and unique impact on rights.*" [36] In a recent Opinion, the Information Commissioner took the view that SWP had not ensured that a fair balance between the strict necessity of the processing of sensitive data and the rights of individuals had been struck.[37]

28. The breadth of public concern around this issue is clear. At the time of writing, Liberty's petition calling for a ban against the use of facial recognition in publicly accessible places had over 12,000 signatories[38], and a statement released in September 2019 by Big Brother Watch was signed by politicians from across the political spectrum and 25 race equality and technology campaign groups – as well as technology academics and legal experts.[39] It is vital that Parliament considers the impact of facial recognition on our fundamental rights and freedoms well prior to the consideration of legislation to regulate its use. Should Parliament be afforded this opportunity, it will be evident that legislation to regulate the use of this technology is insufficient – instead, its use by police in public spaces should be prohibited.

HANNAH COUCHMAN

[36] HC Debate, 15 March 2018, Column 145, Available at: https://hansard.parliament.uk/Commons/2018-03-15/debates/ac095f37-712b-44e1-91bd-78e757ee397e/DataProtectionBill(Lords)(FourthSitting)?highlight=%22facial%20recognition%22

[37] The Office of the Information Commissioner (2019), *Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places,* Reference: 2019/01, Available at: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

[38] See: https://liberty.e-activist.com/page/46698/petition/1

[39] Big Brother Watch (2019), *Joint statement on police and private company use of facial recognition surveillance in the UK*, Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019-1.pdf