Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology

January 2021

The Biometrics and Forensics Ethics Group

Overview

The Biometrics and Forensics Ethics Group (BFEG) was commissioned to investigate the ethical issues raised by the collaborative use of live (real-time) biometric facial recognition technology (LFR) by public (police) and private organisations. This briefing note provides a summary of the evidence gathered by the working group. It focuses on the use of LFR in a range of privately-owned spaces where people are gathered or are passing through (for example, shops and shopping centres) including those with clearly defined transit points where people are 'channelled' past the cameras (for example, within airports). During the evidence gathering process the BFEG Live Facial Recognition Working Group heard from:

- the Metropolitan Police Service;
- Counter Terrorism Policing North East;
- Centre for Data Ethics and Innovation;
- National Crime Agency;
- Biometrics Commissioner's Office;
- Surveillance Camera Commissioner's Office;
- Information Commissioners' Office;
- Big Brother Watch;
- Liberty;
- Anyvision;
- Amazon Web Services (AWS);
- Southern Co-operative Stores; and
- NHS Digital.

Written evidence was submitted by:

- CLUE;
- Hull City Council, CCTV Control Room Manager; and
- the British Security Industry Association.

Summary

In gathering evidence, it was clear that the use of biometric recognition technologies (including LFR) in public–private collaborations (P–PCs) are likely to increase. The BFEG working group highlighted several ethical concerns generated by the collaborative use of LFR, including:

- sharing data and technology;
- the development of behavioural biometrics for use in LFR;
- discrimination and bias in the use of LFR;
- the construction of watchlists; and
- the effect of using LFR in private spaces used by the public.

In the absence of regulation, the working group outlined a number of issues that should be addressed prior to setting up of P–PCs in the use of LFR. The working group also made a number of recommendations that should be followed by those involved in P–PCs, including that an independent ethics group should have oversight of the use of LFR by police forces and in P–PCs.

Introduction and definitions

The use of live facial recognition (LFR) technology raises a number of ethical issues. The Biometrics and Forensic Ethics Group's (BFEG's) 2019 report Ethical Issues Arising from the Police Use of Live Facial Recognition Technology (BFEG, 2019) noted the lack of independent oversight and governance of the use of LFR. It also identified a number of ethical principles that should govern the use of LFR technology by the police, in the absence of a primary (specific) legislative framework. Since that report was published, the use of LFR by South Wales Police (SWP) has been the subject of judicial review in the UK, *R. (Bridges) v. Chief Constable [CC] SWP and the Secretary of State for the Home Department [SSHD]*, 2019 (Royal Courts of Justice Ruling, 2019), the findings of which were subsequently scrutinised by the Court of Appeal (*R. (Bridges) v. CC SWP*, 2020, Court of Appeal, civil division, 2020). The use of LFR by law enforcement agencies has been banned in the State of California (State of California Penal Code §832.19, 2019) and, more recently, a number of technology suppliers – Amazon, IBM, Microsoft – have announced that they are calling a moratorium on the selling of LFR technology to police forces across the world (Amazon, 2020; IBM, 2020; Silicon, 2020). At the same time, the collaborative use of LFR technology in partnerships between the police and private organisations in many parts of the UK, has been highlighted by the media, including: Greater Manchester Police (GMP) and the Trafford Centre (Manchester Evening News, 2018); South Yorkshire Police and Meadowhall Shopping Centre (BBC, 2019a); and the Metropolitan Police Service (MPS) and Argent in King's Cross, London (MPS, 2019, BBC, 2019b), amongst others.

The evidence-gathering process

The BFEG working group received a range of evidence from technology providers, police forces and a number of interested parties including the Information Commissioner's Office, the Biometrics Commissioner, the Surveillance Camera Commissioner, and civil society groups. However, with the exception of the MPS, Counter Terrorism Policing North East and Southern Co-operative Stores, who were prepared to acknowledge their involvement in public–private collaborations (P–PCs), the working group had few real-world examples on which to base the recommendations in this briefing note. Therefore, this note does not provide any details about the specific technologies involved in P–PCs or their methods of implementation. However, as many of those who gave evidence emphasised, **P–PCs in the use of biometric recognition technologies are expected to become more commonplace in the future**.

What is live facial recognition?

In Ethical Issues Arising from the Police Use of LFR technology the BFEG defined LFR as a type of biometric recognition as follows:

“Biometric recognition is the automated recognition of individuals based on their biological and behavioural characteristics, for example, facial image, DNA, voice and gait.

Automated recognition implies that a machine-based system is used for the recognition, either for the entire process or assisted by a human being.

Live facial recognition (LFR) is the automated one-to-many ‘matching’of near real-time video images of individuals with a curated ‘watchlist’ of facial images.

LFR technologies may also incorporate generic object recognition and/or whole body or body part recognition.” (BFEG, 2019)

LFR is typically used to assist the recognition of persons of interest on a watchlist; this means that system operators are required to verify/override a possible match identified by the system (a system alert) and decide what actions, if any, to implement.

What are public–private live facial recognition collaborations?

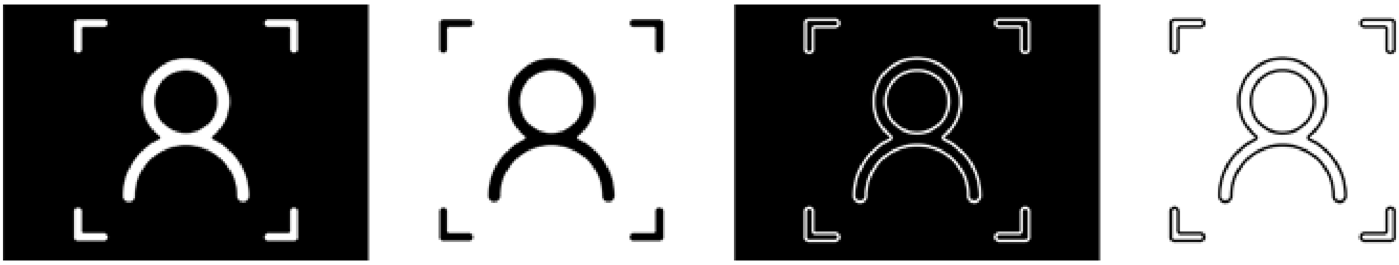
For the purpose of this briefing note, P–PCs are defined as those occasions when both public entities/organisations (such as police forces) and private entities/organisations share data, hardware, software or intelligence for the purposes of LFR. When giving evidence to the working group the civil rights group, Liberty, described the three main scenarios involving P–PCs.

1. The police provide private owners of LFR with a digital watchlist of persons of interest (for example, missing persons, persons suspected of committing a crime). This is used in a privately-owned space frequented by members of the public (for example, a shopping centre).

2. A match is generated by a privately operated LFR system using a privately curated watchlist, that may indicate a need for police intervention. For example, a group of shops have LFR technology and collect and share images of suspected shoplifters, one of whom is identified by the system executing a crime and the police are asked to arrest the suspect.

3. A private company sells LFR software to a police force. [Of note, the private company may also sub-contract or outsource different aspects of the system, for example, the platform, data storage, and algorithms may be provided by third parties beyond the primary P–PC].

This briefing note focuses on the first two scenarios, which involve real-time collaborative deployment of LFR technology. In the course of hearing evidence from public and private authorities, the BFEG working group heard about many forms of collaboration between public and private authorities using LFR technologies. Most of these could not accurately be described as partnerships, in the sense of a clearly defined formal or contractual relationship between two parties. However, they all involve collaboration, which means that there is a flow of data, computational infrastructure (hardware, software, platforms) and knowledge that crosses public–private boundaries.



The impact of R. (Bridges) v. Chief Constable of South Wales Police on public–private collaborations

While the working group was gathering evidence for this report the Court of Appeal handed down its judgment in *R. (Bridges) v. Chief Constable of South Wales Police* [2020](Court of Appeal, civil division, 2020). The Court held that the use of LFR technology by the SWP in some field trials was unlawful. The Court made this determination on three main legal grounds (see Box 1). While the remit of this briefing note is wider, namely, to look at collaborative uses of LFR, this judgment also has implications for the uses of LFR in P–PCs, thus, our recommendations should be read alongside this recent ruling.

Box 1: The legal issues in the use of live facial recognition by South Wales Police identified in the *R. (Bridges)* case	
1	The use of the automated facial recognition (AFR) system was held to have breached the right to respect for private life protected by the UK Human Rights Act 1998 because the court found critical defects in the legal framework that left too much discretion to individual officers.
2	The AFR system had breached Section 64 of the Data Protection Act 2018 on the basis that the Data Protection Impact Assessment had *"failed properly to assess the risks to the rights and freedoms of data subjects and failed to address the measures envisaged to address the risks arising from the deficiencies we have found".* This included two *"impermissibly wide areas of discretion"*; the selection of those on watchlists; and the locations where AFR may be deployed.
3	South Wales Police (SWP) was in breach of its public sector equality duty (PSED) under section 149 of the Equality Act 2010 in that *"SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex".*

Ethical concerns

As public and private organisations increasingly collaborate in the development and deployment of live facial recognition (LFR) technologies a number of key issues need to be addressed. Many of these involve general questions about data uses – for example, how data are generated, who can access and share them, what are the purposes of data sharing and what are the ethical benefits and risks? As well as some more specific ethical concerns, such as:

The sharing of data and technology: A number of public-private collaborations (P-PC) in the use of LFR have involved the police supplying a 'watchlist' of facial images (i.e. data) to private organisations (for example, the Metropolitan Police and British Transport Police to King's Cross Estate (Argent); South Yorkshire Police to Meadowhall shopping centre (British Land); and Greater Manchester Police to the Trafford Centre (INTU)).

The machine learning processes used in LFR systems mean that it is not just images that are shared by collaborators, but a biometric 'feature space' (a collection of features used to characterise the data Trigueros et al., 2018), which can be combined and processed with other data sources. P–PCs not only share images/data, but may also share machine learning tools, deep neural network algorithms, training datasets, and so on. For example, the providers of the LFR technology could use data collected during P–PCs to train or refine their algorithm.

As the Biometrics Commissioner observed during the evidence gathering, P–PC in the training and testing of algorithms means that datasets collected for one purpose (and by one organisation) are repurposed for processing in a new way by another organisation, which has implications for the data subjects' rights and may violate data protection law. However, it must be noted that many facial recognition tools (including for example, Amazon Rekognition) allow individuals configuring the service for a given implementation to choose whether image data captured by their implementation are used for training purposes or not – in other words, this data-sharing feature can be turned on or off.

Live facial recognition and behavioural biometrics: LFR technologies are rapidly evolving and combining with other biometric modalities (for example, movement/gait). The collaborations with private organisations are crucial in this respect because private organisations are extending and expanding what public authorities can do with these technologies. The use of facial recognition tools alongside other software tools could allow police forces and private entities to analyse different forms of data concurrently, for example, video data containing facial images can be analysed alongside many other forms of data (social media and immigration data). In this model LFR can be merged with other machine learning techniques such as: text extraction, object recognition, and sentiment analysis (for example see AWS, 2020). As a result, LFR technologies are no longer confined to biometric face matching, but can be used as part of wider systems for risk-based profiling and the inference of behaviour in public spaces. In short, the use of cloud-based platforms ensures that many data types from many public and private sources can be used in machine learning models without any actual 'sharing'.

Discrimination and bias in public–private collaborations: The issues of racial discrimination and bias within LFR technologies have been widely acknowledged (BFEG, 2019; Buolamwini and Gebru, 2018; NIST, 2019; Global Privacy Assembly, 2020). The advent of P–PC has the potential to exacerbate discrimination and bias, particularly in cases where a public authority does not scrutinise the private entity's training dataset and algorithm testing. For example, the individual's rights under data protection legislation (Data Protection Act, 2018; General Data Protection Regulation, 2016) are particularly challenged if it is unclear whether a private entity's LFR technology is biased or inaccurate and is storing individual's data as a result of incorrect matches. Moreover, in the R. (Bridges) case the Court of Appeal held that SWP was in breach of its public sector equality duty because it had not satisfactorily addressed the potential for, algorithmic bias in the LFR technology used in its field trials. This led the Court to raise questions regarding the lawfulness of the police using LFR systems designed by private manufacturers that do not allow for the testing of their software in order to ensure that it is free of racial and gender bias (Court of Appeal, civil division, 2020).

Furthermore, as seen below, when compilation of the watchlist involves both public and private organisations a range of people can add images to the watchlist, and this potentially increases the number of points where discriminatory assumptions can enter the use of LFR technology. In sum, there is profound difficulty associated with tracing the amplification of bias and discrimination in data/algorithms when they cross public and private entities (often many times).

Watchlist construction: The construction of watchlists raises a number of issues:

- the size of the list;
- who is included; and
- who should be responsible for the list's construction.

The National Police Chief's Council and the College of Policing are compiling guidelines on the construction and management of watchlists for use by police forces, however, when this report was written there were no published guidelines in the UK on:

- the types of people who should be included on watchlists;
- what counts as the optimum size of watchlist from an ethical or logistical point of view; and
- who should have responsibility for creating and managing watchlists.

During evidence gathering the Surveillance Camera Commissioner emphasised that P-PCs in the use of LFR are increasing and in his recent report, Facing the Camera (SCC, 2020), he urged that those working in P-PCs using LFR should "aspire to the highest ethical, procedural and legal standards" in these collaborations, particularly in the management of watchlists. The report also notes that police forces in England and Wales involved in P-PCs using LFR should adhere to the Surveillance Camera Code of Practice (2013) and that, while the terms of a specific P-PC may not require a private organisation to abide by the Code, their voluntary adoption of the Code should be encouraged.

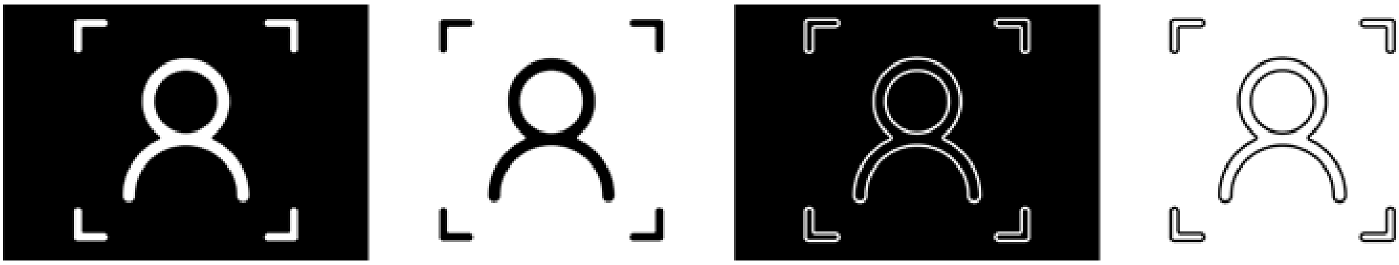
In the private sector watchlist creation, curation and management may vary between organisations. For example, in the Southern Co-operative Stores' trial of LFR the watchlists were created and managed centrally from images taken from incidents reported at individual stores (see also Facewatch, 2020). Alternatively, software providers, such as CLUE, may provide their users access to a database of people suspected of shoplifting collated from CCTV images and photos uploaded by other users.

Issues concerning the construction of watchlists in the SWP trials were noted in the *R. (Bridges)* judgment when the Court of Appeal held that it was "not clear who can be placed on the watchlist" and that criteria for inclusion on watchlists were too subjective and very broad. Finally, the Court of Appeal observed there was "too broad a discretion vested in the individual police officer to decide who should go onto the watchlist" and also highlighted the fact that no particular rank of police officer was required to authorise deployment of this technology.

Freedom to use privately owned spaces: At the cutting edge of machine learning methods for facial recognition, computer scientists are training neural network algorithms to recognise partially concealed faces (Abhila and Sreeletha, 2018). During evidence gathering it was found that LFR technologies are being updated in response to the wearing of face coverings during the COVID-19 pandemic. Developments such as this are making it more difficult for people to exercise their agency to 'opt out' of surveillance (Independent, 2019), with the result that there may be a 'chilling effect' as people may no longer feel free to gather in or enter locations where LFR is in use. P–PCs in LFR extend and deepen the reach of this form of surveillance, particularly in spaces that are privately owned, but used by the public (for example, shops, shopping centres, the King's Cross estate).

Where the images of individuals understood to be 'vulnerable' or at risk (for example, a small child walking alone in a shopping centre) or deemed a risk to a private organisation (for example, individuals suspected of repeated shoplifting) are more likely to be collected and retained, this may lead to a disproportionate number of people being targeted on the basis of a protected characteristic (for example, age, disability, sex, sexual orientation, race) as defined by the Equality Act (2010, chpt 1).

Finally, the growing use of LFR technology in public spaces was also noted in the *R. (Bridges)* judgment, in which the Court held that there were also "*fundamental deficiencies*" in the legal framework concerning the criteria for determining where automated facial recognition can be deployed. The Court noted that the SWP's deployment of LFR at "all event types ranging from high-volume music and sporting events to indoor arenas" was "very broad and without apparent limits".



Issues that should be addressed prior to the use of LFR in public–private collaborations.

The Biometrics and Forensic Ethics Group (BFEG) believes that the use of live facial recognition (LFR) in public–private collaborations (P–PCs) raises a number of issues, beyond those outlined in its earlier report (BFEG, 2019); these are briefly outlined below. In the absence of any specific regulation governing the use of biometric recognition technologies for law enforcement purposes, specifically those involving P–PCs, the BFEG suggests that the following should be addressed prior to the collaborative use of LFR:

Demonstrate that the collaboration is necessary

It is generally not permitted for the police to share information about members of the public with private organisations. Any deviation from this fundamental ethical principle can be justified only if it serves an important public interest that could not be achieved without this collaboration. If the police cannot discharge their responsibilities without collaborating with private organisations, then the data or information that are shared by the police or indeed, by private organisations with the police in these collaborations, should be only what is necessary for the police to perform their role (the ‘necessity condition’).

Demonstrate that the data sharing required in the collaboration is proportionate

The benefits to policing must be sufficiently great to justify any loss of privacy involved in the sharing of information either by the police or by private organisations with the police. That is, it must be proportionate (the ‘proportionality condition’).

Define the types of data that are being shared in the collaboration

Images should be shared as vectors or encrypted vectors so that they cannot be interpreted until a match occurs. Other biometric transactions between collaborators may also take place, for example, the sharing of metadata concerning image quality, match-scores and information on camera performance. In addition to clarifying what types of data are shared, collaborators should confirm when data are shared and for how long (i.e. when they are/will be deleted from the system).

Recommendations

Public–private collaborations (P–PCs) in the use of biometric recognition technologies, including live facial recognition (LFR), are predicted to grow over the next few years. The sharing of data/ technology between the private and public sectors raises a number of ethical issues over and above those generated by public (police) sector use of LFR.

In the absence of a legislative framework governing the use of LFR by the police or in P–PCs, the Biometrics and Forensic Ethics Group (BFEG) makes the following recommendations.

1. **Police should only share data with trustworthy organisations that have been vetted.**

The police should only share data with trustworthy private organisations. Members of private organisations who will have access to police data should be vetted for their trustworthiness.

2 **Data should be shared with, or accessed by, the minimum number of people.**

All public and private data should be shared with the minimum number of people. This means that suppliers of LFR technology should not be able to access the images/data compiled in a watchlist or the results of biometric transactions and image metadata for refining algorithms or other purposes.

3 **Biometric data (including image data) must be safely and securely stored.**

Arrangements should be made for the safe and secure sharing and storage of data (including associated metadata) in P–PCs, such as those outlined in the Information Commissioner's Office's (ICO's) Data Sharing Code of Practice (ICO, 2020, Security). Data should not be stored for any longer than is necessary.

4 **Watchlists should be narrow and targeted.**

Private and public watchlists should be narrow, targeted and proportionate to the deployment to avoid the oversharing of personal data between private and public organisations.

5 **A publicly accessible record of collaborative uses of LFR should be created.**

To ensure transparency, P–PCs should be publicly recorded for example, on the police force website, which documents for each deployment:

- the purpose of the collaboration;
- the identity of the collaborators; and
- the types and amount of data that are being shared, with whom and for how long.

For example, Force A is collaborating with private organisation B by providing N images/ records, which are stored for X time and will used by Y actors now and in the future.

6 **Collaborative use of LFR should be authorised by a senior police officer**.

P–PCs should proceed only if they have been authorised by a senior police officer (Superintendent or above).

7 **An independent ethics group should oversee the use of LFR by the police and in P–PCs .**

To maintain public confidence, the BFEG recommends that oversight mechanisms should be put in place. The BFEG suggests that an independent ethics group should be tasked to oversee a) individual deployments of biometric recognition technologies by the police and b) the use of biometric recognition technologies in P–PCs. This independent ethics group would require that any proposed deployments and P–PCs are reviewed when they are established and monitored at regular intervals during their operation.

Authors

The main authors of the report are members of the Facial Recognition Working Group of the Biometrics and Forensic Ethics Group: Nina Hallowell (Chair 2019 to January 2021), Louise Amoore (Chair from January 2021), Simon Caney, Richard Guest and Peter Waggett, with additional contributions on legal analysis from Dr Nóra Ni Loideain. The report has been ratified by all members of the Biometrics and Forensic Ethics Group (see Appendix 1 for a list of members).

References

Abhila, A. G. and Sreeletha, S.H. (2018) 'A Deep Learning Method for Identifying Disguised Faces', *International Research Journal of Engineering and Technology*, vol. 5 (7), pp 1239–1244. Available at: https://www.irjet.net/archives/V5/i7/IRJET-V5I7222.pdf [accessed 7 September 2020].

Amazon (2020) 'We are implementing a one-year moratorium on police use of Rekognition', Amazon news, June 2020. Available at: https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [accessed 7 September 2020].

AWS (2020) 'Automatically detecting personal protective equipment on persons in images using Amazon Rekognition', Amazon Web Services, October 2020. Available at: https://aws.amazon.com/blogs/machine-learning/automatically-detecting-personal-protective-equipment-on-persons-in-images-using-amazon-rekognition/ [accessed 27 October 2020].

BBC (2019a) Meadowhall shoppers scanned in facial recognition trial, BBC News, 16 August 2019. Available at: https://www.bbc.co.uk/news/uk-england-south-yorkshire-49369772 [accessed 6 November 2020].

BBC (2019b) Met Police gave images for King's Cross facial recognition scans, BBC News, 6 September 2019. Available at: https://www.bbc.co.uk/news/technology-49586582 [accessed 6 November 2020]

BFEG (2019) *Ethical Issues Arising from the Police Use of Live Facial Recognition Technology*, Biometrics and Forensic Ethics Group. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf [accessed 7 September 2020].

Buolamwini, J. and Gebru, T. (2018) 'Gender Shades: Intersectional Accuracy in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81, pp 1–15. Available at: http://proceedings.mlr.press/v81/buolamwini18a.html [accessed 7 September 2020].

Court of Appeal, civil division (2020) *R. (Bridges) v. Chief Constable of South Wales Police*. Available at: https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html [accessed 21 October 2020].

Data Protection Act (2018) [online]. Available at: https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted [Accessed 7 September 2020].

Facewatch (2020) 'Facewatch at the Southern Co-op', 5 October 2020. Available at: https://www.facewatch.co.uk/2020/10/05/facewatch-at-the-southern-co-op/ [accessed 6 November 2020].

General Data Protection Regulations (2016) Available at: https://www.legislation.gov.uk/eur/2016/679/contents [Accessed 7 September 2020].

Global Privacy Assembly (2020) *Adopted Resolution on Facial Recognition Technology*, 42nd Closed Session of the Global Privacy Assembly. Available at: https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf [Accessed 22 October 2020].

IBM (2020) 'IBM CEO's Letter to Congress on Racial Justice Reform', 8 June 2020. Available at: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/ [Accessed 7 September 2020].

ICO (2020) Data Sharing Code of Practice, Information Commissioner's Office. Available at: https://ico.org.uk/for-organisations/data-sharing-information-hub/ [Accessed 7 January 2021]

Independent (2019) 'Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested', 31 January 2019. Available at: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html [Accessed 7 September 2020].

Manchester Evening News (2018) 'Trafford Centre bosses explain why they used controversial cameras to monitor shoppers', 15 October 2018. Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/trafford-centre-bosses-explain-used-15283677 [Accessed 7 September 2020].

Metropolitan Police Service (2019) Report to the Mayor of London, Sept 2019. Available at: https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf [Accessed 11 January 2021].

NIST (2019) Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [Accessed 11 January 2021].

Royal Courts of Justice Ruling (2019) EWHC 2341 R. *(Bridges) v. Chief Constable of South Wales Police and Secretary of State of the Home Department*. Available at: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf [Accessed 7
September 2020].

Silicon (2020) 'Microsoft Bans Facial Recognition Sales to Police', Silicon newsletter, June 2020. https://www.silicon.co.uk/e-innovation/artificial-intelligence/microsoft-bans-facial-recognition-police-345703 [Accessed 7 September 2020]

Surveillance Camera Code of Practice (2013) Available at: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice [Accessed 11 January 2021].

Surveillance Camera Commissioner (2020) '*Facing the Camera*'. Available at: https://www.gov.uk/government/publications/police-use-of-automated-facial-recognition-technology-with-surveillance-camera-systems [Accessed 11 January 2021].

Trigueros, D. S., Meng, I. and Hartnett, M. (2018) 'Face Recognition: From Traditional to Deep Learning Methods'. Available at: https://arxiv.org/pdf/1811.00116.pdf [Accessed 7 September 2020]

Appendix 1: Membership of the Biometrics and Forensics Ethics Group

The BFEG is an advisory non-departmental public body, sponsored by the Home Office. The group provides advice on ethical issues in the use of biometric and forensic identification techniques such as DNA, fingerprints, and facial recognition technology. The BFEG also advises on ethical considerations in the use of large and complex data sets and projects using explainable data-driven technology.

Chair

Professor Mark Watson-Gandy, a practising barrister at Three Stone Chambers and Visiting Professor at the Universities of Westminster and Lorraine.

Committee members

Dr Adil Akram, Consultant Psychiatrist, South West London and St George's Mental Health NHS Trust and Honorary Senior Lecturer, St George's, University of London

Professor Louise Amoore, Professor of Human Geography, Durham University

Professor Liz Campbell, Chair in Criminal Jurisprudence, Monash Law, Australia

Professor Simon Caney, Professor in Political Theory, University of Warwick

Professor Richard Guest, Professor of Biometrics Systems Engineering and Head of the School of Engineering and Digital Arts, University of Kent

Professor Nina Hallowell, Professor of Social and Ethical Aspects of Genomics, University of Oxford

Dr Julian Huppert, Director and Fellow, Intellectual Forum, Jesus College, Cambridge

Professor Mark Jobling, Professor of Genetics, University of Leicester

Dr Nóra Ni Loideain, Director of the Information Law and Policy Centre, Institute of Advanced Legal Studies, University of London

Isabel Nisbet MPhil BPhil MA, Board of Qualifications Wales and Board of Governors, University of Hertfordshire and University College of Osteopathy. Affiliated Lecturer, Faculty of Education, University of Cambridge.

Professor Charles Raab, Professorial Fellow, University of Edinburgh and Turing Fellow, Alan Turing Institute

Professor Tom Sorell, Professor of Politics and Philosophy, University of Warwick

Professor Denise Syndercombe-Court, Professor of Forensic Science, King's College London

Professor Jennifer Temkin, Professor of Law, The City Law School (City University of London)

Dr Peter Waggett, Director of Research, IBM