College of Policing

Working together
to give policing a voice

Consultation on

Live facial recognition

Authorised Professional Practice

Feedback form

Consultation closes 27 June 2021

About this consultation

We want to hear your views on our draft document of the live facial recognition (LFR) Authorised Professional Practice (APP).

The guidance will be of particular relevance to chief officers and will also be of interest of those working in information management.

LFR is a real-time deployment of facial recognition technology. It compares a live camera feed(s) of faces against a predetermined watch list to locate persons of interest by generating an alert when a possible match is found. The APP provides guidance to forces to operate LFR technology in pursuit of policing objectives.

Please use this form to send us your feedback. The feedback boxes will increase in size as you enter your text.

Send your completed form to:
LFR_Consultation@college.pnn.police.uk

Please respond no later than **27 June 2021**.

All feedback will be collated and analysed by College staff and the draft APP amended if appropriate. We will only contact you if we need to clarify any of your comments and you give us your contact information. A summary of changes made as a result of feedback will be published at the same time as the final APP.

Privacy notice

The information you have provided will be held by the College of Policing in accordance with data protection legislation. Your information will be lawfully held and processed for the purposes of informing the consultation phase of APP development.

The information will be processed under the lawful basis of public task.

The information you provide will only be used to inform development of the product.

Your personal information may be shared with internal business units and force subject matter experts when analysing feedback.

Your personal information will not be shared outside of this process.

We will hold your information for one year. After this period your information will be securely disposed of.

The College takes its data protection responsibilities very seriously. Your information will be held securely and will only be processed for the purposes stated above or to fulfil a statutory obligation.

You have certain rights under data protection legislation regarding your personal information. These include the right to access information held about yourself, to ensure it is accurate and to ask for it to be deleted or no longer processed.

For more information about your rights, please see our full privacy notice, which can be found on the legal page of our website. You can also contact our data protection officer by emailing: **Data.Protection@college.pnn.police.uk**

About you

Name (optional)	*Ed Geraghty, Emmanuelle Andrews, Jen Persson, Sahdya Darr, Silkie Carlo*
Role (optional)	Click here to enter text.
Organisation (optional)	*Privacy International, Liberty, Defend Digital Me, Open Rights Group and Big Brother Watch*
Please tell us if your views are personal or whether they represent an official response from your organisation. If official, please state in what context (eg, chief constable, head of information).	*The content below represents the views of above organisations*
If you are willing to be contacted should we need further clarification on your comments, please provide your contact details.	Click here to enter text.
If you wish to be informed when the final APP is published, please provide your contact details.	Click here to enter text.

Consultation questions

It will be helpful for us to understand why you have given a particular answer, or how you think the APP could be improved. Please provide detailed comments wherever possible.

1. To what extent do you think the APP is easy to follow and understand? Please let us know if there are any specific changes you would like to see.

Privacy International, Liberty, Defend Digital Me, Open Rights Group, and Big Brother Watch welcome the opportunity to submit a joint response to the College of Policing's public consultation on national guidance for live facial recognition technology (LFRT).

As a point of principle, all the aforementioned organisations believe that LFRT poses significant and unmitigable risks through police use of LFRT.

Whilst we engage with the below questions, we do not believe that LFRT can ever be safely deployed in public spaces. We therefore believe that LFRT, whether in use by police or private companies, should be prohibited entirely.

While overall the APP can be followed and understood with relative ease, the seemingly clear wording obscures the elephant in the room – this APP appears to be an attempt to bypass parliamentary scrutiny and debate. The intrusiveness of LFRT and the dangers associated with its potential abuse by the police call for robust safeguards and oversight governing its authorisation and use, should it ever be deemed permissible.

Against a backdrop of little Parliamentary scrutiny on this significant step change in policing, it is essential that Members of Parliament and Peers demand the opportunity to steer the debate. Whether and how live facial recognition is used by our police forces – a move which

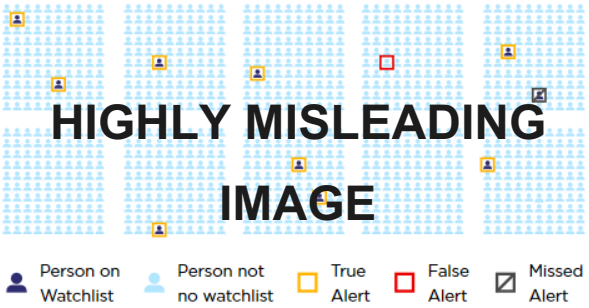
fundamentally alters the relationship and balance of power between us and the State – should be set down in primary legislation and subject to Parliamentary scrutiny.

We further note that MPs in the House of Commons Science and Technology Committee called for the police use of LFRT to be suspended until further legislative framework is applied to the technology.[1]

It is also dangerous, as we see in Section 4 *"Key Performance Metrics"*, to simplify language when it comes to mathematics and statistics.

The simplification of the language in this section obscures the realities of the deployments to date – of those stopped as a result of human-adjudicated alerts, consistently **2/3rds of stops under LFRT are verified incorrect matches**[2].

Simplifying language to talk about 'accuracy' and using ratios without absolute numbers is simplification to the extent of being misleading.



The image used in 5.2.22 (reproduced left) takes that one step further, given trials to date demonstrate **2 out of every 3** stops have been a 'Confirmed False Alert'[2] – i.e. following engagement, it is determined that the engaged individual is not the same as the person in the candidate image in the watchlist – not 1/10 as this image implies (the image only shows one red square as false alert). This is problematic and we would welcome more detail from the

[1] UK House of Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session 2017–19 (HC 1970, 18 July 2019) https://www.publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003

[2] Fussey, Peter and Murray, Daragh (2019) Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Project Report. University of Essex Human Rights Centre https://repository.essex.ac.uk/24946/

College of Policing surrounding the research that has been undertake to arrive at such an incorrect image.

There were also a number of 'credible matches' not able to be 'verified' by a stop. Indeed, these numbers appear to be roughly equal to those stopped overall[2]. It is impossible to know whether these 'matches' were correct – or, indeed whether 'matches' deemed 'non credible' would in fact have been correct had the 'match' been 'verified', further complicating any notion of 'accuracy' around this technology. We believe it is misleading to include those matches within the 'credible matches' category.

Finally, we cannot know the 'missed alert' rate without seeding a 'blue watchlist' – something your guidance makes clear (4.1.5) should not be focused on 'as it may increase the false alert rate to an extent that is not possible to manage the number of false alerts'. We also reiterate that even if the misleading accuracy readings are adjusted, this does not imply that this will make the use of LFRT acceptable. As stated above, all the aforementioned organisations strongly object to the use of LFRT by the police due to its significant and unmitigable risks to individual liberties.

2. To what extent do you think the guidance in the APP provides a clear legal and ethical framework for forces to operate LFR technology in pursuit of policing objectives? Please let us know if there are any specific changes you would like to see.

The guidance in the APP does not provide a clear legal and ethical framework for forces to operate LRF technology in pursuit of policy objectives. The guidance fails to take account of the judgment in *R (Bridges) v Chief Constable of South Wales Police & Ors.* In fact, the guidance is similar to the very framework the Court criticised in R(Bridges).

We reiterate that if the police seek to use LFRT it must be introduced via primary legislation and subject to Parliamentary scrutiny. Reliance on common law 'policing duties' (1.1.2 & 1.1.3) is unacceptable. It avoids clear and accessible legislative frameworks.

We do not accept that LFRT can be viewed as a technology solely designed for 'preventing or detecting crime'. This is a highly intrusive

technology going far beyond what we may call 'traditional CCTV' (the efficacy of CCTV in preventing or detecting crime is itself controversial, although outside the purview of this document).

Given deployments to date have seen 3 times as many people stopped as should have been, and have seen several escalating confrontations between police officers and members of the public exercising their right to not consent, we question the effectiveness in LFRT being justified to 'preserve order'. Given the poor matching it appears comparatively ineffective in seeking to 'bring offenders to justice' than regular police availability. We are not aware of a cost benefit analysis in this respect.

The APP further refers to several other documents which must be taken into account, including the *Surveillance Camera Code of Practice*, which states:

"The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and *such consent on the part of the community must be informed consent and not assumed by a system operator. Surveillance by consent should be regarded as analogous to policing by consent.* In the British model of policing, police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so."

We have seen in trials to date individuals having been stopped as a result of 'suspicious behaviour' such as covering their faces from the LFR cameras. The College of Policing must make it clear officers must not stop individuals simply because they want to protect their biometric identities. We are glad 1.4.4(b) reminds police that 'in normal circumstances […], the police do not have a legal power to require persons to remove clothing simply because they are passing the LFR system'.

The guidance fails to provide the clear legal framework required by the Bridges judgment, in respect of both the watchlist and where LFRT is

deployed. For example, in our view it does not preclude the use of LFRT for intelligence gathering purposes, which the Court found was an impermissibly wide discretion. We are also concerned that the guidance does not limit the watchlist to photos obtained lawfully by the police, and allows police forces to use photos obtained from social media or third parties. The categories of individuals who may be added to watchlists – going as far as victims of and witnesses to crime – appears difficult to justify.

We welcome that the guidance identifies locations which raise a greater expectation of privacy, but in our view, there are no circumstances in which LFR should be deployed in the locations identified - outside hospitals, schools, or places of worship.

Further, whilst the guidance draws specific attention to protected characteristics (2.2), and we welcome the acknowledgement that 'Scientific opinion indicates that the accuracy of facial recognition may be influenced by the data sets used to train its capabilities', particularly with 'faces of [ethnic minority] demographics', there appears to be little to no real engagement with how this can actually be addressed.

As commented in *Bridges*: 'In order to check the racial or gender bias in the technology, [the racial or gender profiles of the total number of people who were captured by the LFR technology but whose data was then almost immediately deleted] would have to be known. We accept [..] that it is impossible to have that information, precisely because a safeguard in the present arrangements is that that data is deleted in the vast majority of cases.'.

This is compounded by 'the precise makeup, scale and sources of the training data used [being] commercially sensitive' meaning that, even to a court, it 'cannot be released'. In our view, the guidance should discourage forces from procuring software where there are constraints on analysing the underlying data, or at least make explicit that commercial secrecy cannot be relied on for any failure to understand inbuilt bias.

In the absence of information provided by manufacturers, it cannot be for Constabularies to audit the efficacy of these 'commercially sensitive' algorithms, without running their own trials. There is no practical assistance for police in how to conduct such trials. For example, given the poor recognition of ethnic minority faces, to ensure efficacy it would be required for these algorithms to be disproportionately trained on images of ethnic minorities. Further if the Police do attempt to conduct their own audits, the audit's independence would be

compromised.

There is a failure to consider the impact of the use of LFRT on children.

The questions of differentiation between the age of a child is raised by the under / over 13 split in paragraph 2.2.3. This is an arbitrary and artificial divide in so far as it is a generalisation and the purpose of the divide at 13 is not immediately clear since accuracy such as raised in 2.2.5 is an individual question in each case for any child, not age dependent.

In the Information Commissioner's Opinion on the use of live facial recognition technology by law enforcement in public places[3], there is no mention of children and this College of Policing Consultation makes no attempt to address the impact on children either.

It is reported that children are a population over-policed through CCTV and research has found[4] that that the effects on children of pre-emptive surveillance are wide-ranging and rarely addressed.

The Policing Crime Sentencing and Courts Bill[5] will bring more children into the criminal justice system through the changes on protest and those affecting the Traveller community and the applications of LFR in any of these contexts is open to scope creep.

In Scotland, there is extensive work going on in policing and across the public sector which examines the adoption of the UN Convention on the Rights of the Child (UNCRC) and the implications for domestic law, in respect of for how children are treated in interactions with the State (https://www.gov.scot/policies/human-rights/childrens-rights/). This consultation by contrast, fails to attempt to understand this or the impact of its approach.

[3] Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places - 31 October 2019 - **https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf**

[4] Surveillance Futures. Social and ethical implications of new technologies for children and young people (2017) Eds. Emmeline Taylor and Tonya Rooney, Routledge. Van Brakel, R. (14) Rise of Pre-emptive Surveillance

[5] **https://bills.parliament.uk/bills/2839**

Therefore, while our principal position is that it is inappropriate to use LFRT at all, we recommend a Child Rights Impact Assessment of LFR should be carried out, as well as DPIA, mindful of this apparent changing direction of travel for policing children.

Finally, there is no acknowledgement within the guidance that the public sector equality duty applies not only to the technology itself, and the datasets it is trained on, but also to the images included on the watchlist and the communities within which it is deployed.

3. How easy or difficult do you think it will be to implement the APP across forces if they choose to use LFR technology?

As we have made clear throughout our responses, the premise that LFRT can be deployed by forces choosing to use 'LFR technology' without the introduction of primary legislation which would subject to primary legislation is wrong. We maintain LFRT should never be deployed. Nevertheless, any legal framework must be publicly accessible, clear, precise, comprehensive and non-discriminatory. Reliance upon the AAP falls short.

Constabularies historically have a poor record when it comes to paper trails, even with basic legal requirements such as DPIAs[6].

We believe it would be quite difficult to achieve consistency of implementation of the APP, as it is vague in many places and leaves a lot of crucial decisions to the 'forces' themselves. As a result, this could lead to numerous inconsistencies between 'forces' as to how the code is applied and how any purported the safeguards are implemented.

As the Court said in Bridges, "*It may be prudent, however, for there to be at least consistency in the content of local policies…*" Further, the lack of any requirement to publish policies makes it very difficult to see how the legal framework required by Bridges will be reasonably accessible or foreseeable to the public, which it must be in order to be lawful.

[6] https://www.computerweekly.com/news/252493673/UK-police-unlawfully-processing-over-a-million-peoples-data-on-Microsoft-365

4. Do you have any suggestions that you think would help the implementation of the APP?

The APP begs the question, presupposing LFRT can ever be lawfully or ethically deployed.

In a democratic society, it is imperative that such intrusive and chilling technologies are given proper parliamentary scrutiny.

They must not be allowed to be used in legal 'grey areas' – particularly when the legal justification relied on in this APP is practically indistinguishable to that judged insufficient in Bridges.

5. Do you have any other comments on the draft APP?

Police use of live facial recognition technology in public spaces is an enormous infringement of privacy for everyone who passes by the camera.

We are concerned that deployments of this surveillance technology could mirror and exacerbate existing disproportionate policing practices. For example, it has been reported that the Met police 'disproportionately' use stop and search powers on black people[7]. Amnesty International reported[8] on the 'Gangs Matrix' which it called a racially discriminatory system that stigmatises young black men for the music they listen to or their behaviour on social media.

[7] https://www.theguardian.com/law/2019/jan/26/met-police-disproportionately-use-stop-and-search-powers-on-black-people
[8] https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police

More generally, 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. In some cases, identification determines how the State interacts with people and whether they are afforded access to their rights.

The rapid advances in the field of artificial intelligence and machine learning, and the deployment of new technologies that seek to analyse, identify, profile, and predict, by police, have and will continue to have a seismic impact on the way society is policed. The use of facial recognition represents a huge shift in the relationship between the individual and the State, and for our right to remain anonymous more broadly. The implications come not solely from privacy and data protection perspectives, but from the ethical question for a democratic society of permitting the roll out of such intrusive technology.

"A person's face is a precious and fragile element to her identity and sense of uniqueness. It will change in appearance over time and she might choose to obscure or cosmetically change it – that is her basic freedom. Turning the human face into another object for measurement and categorisation by automated processes controlled by powerful companies and governments touches the right to human dignity – even without the threat of being used as a tool for oppression by an authoritarian state. Moreover, it tends to be tested on the poorest and most vulnerable in society, ethnic minorities, migrants and children."[9]

The technology violates our dignity and contradicts the essence of our rights. It unacceptably weakens the core of several freedoms, and casts a chilling effect on society by imposing a sense of constant surveillance, (self) restriction, censoring and criticism, and normalises authoritarian surveillance.

[9] EDPS, Facial Recognition: A solution in search of a problem? (28 October 2019) https://edps.europa.eu/press-publications/press-news/blog/facial-recognition- solution-search-problem_en

This APP is an attempt to side-step the debate, discussion, parliamentary and legal oversight such intrusive technologies must be given in a democratic society.

Nonetheless, Privacy International, Liberty, Defend Digital Me, Open Rights Group and Big Brother Watch believe that even if there were laws regulating the use of this technology, it would still pose an unacceptable threat to human rights and should have no place in our public spaces.

Send your completed form to: **LFR_Consultation@college.pnn.police.uk**

About the College

We're the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

college.police.uk