Match up: Facial recognition technology and public expectations

The Ada Lovelace Institute welcomes the Justice Sub-Committee on Policing’s contribution to growing policy discussion of facial recognition technology.

Our response is founded on evidence from our research with the public undertaken in July 2019, summarised as two questions and a recommendation for 2026 strategy, which we elaborate on below:

1) Do police have ‘carte blanche’ in making use of facial recognition technology?
2) Can police demonstrate public benefit and assurance of safeguards?
3) There is a need to pause and take stock of how facial recognition will be applied, for greater clarity on scenarios and preparation for their adoption into practice.

Introduction

The Ada Lovelace Institute, funded by the Nuffield Foundation, is an independent research organisation established in 2018 with a mission to ensure that data and AI work for people and society.

Our first published report presents the results of a nationally representative survey of 4,109 of the UK public, undertaken with YouGov, on public attitudes to facial recognition technology. The survey sought to measure public views on a selection of brief examples and use cases that show how the technology is increasingly being applied in a variety of ways, for different purposes, in both the public and private sectors.

As next steps, we are:

- forming a new national assembly of citizens, the Citizens Biometrics Council, to hear evidence and debate over the benefits articulated, how those benefits are assured, and what would constitute ‘red lines’ or publicly unacceptable risks
- reviewing the forms that governance over facial recognition, digital recognition and identity technologies can take

---

• engaging with parliamentary and government bodies, police forces, and legal and governance experts in this domain.

1) Do police have a ‘carte blanche’ (unlimited discretionary power to act) in making use of facial recognition technology?

Our work, and the broader evidence base on facial recognition technology, strongly indicates that the public's somewhat higher awareness of and support for the technology's use in policing should not be taken as a ‘carte blanche’. The technology’s worth should be subject to tests and measurable by much more than public opinion.

With regard to public sector policing, the major finding of our national public survey was that people fear the normalisation of surveillance, but are prepared to accept facial recognition technology when there is a clear benefit.

Nearly half (49%) support the use of facial recognition technology in day to day policing, assuming appropriate safeguards are in place.

71% agree with the statement ‘The police should be able to use facial recognition technology in public spaces, provided it helps reduce crime’.

We saw a much stronger trend of public objection and protest in some other cases. The use of facial recognition technology to register pupils in schools might not be deemed fundamentally worthwhile. Uses by companies also showed lower levels of support; suggesting to us that the public does not trust the private sector to use facial recognition technology ethically. Other and wider research similarly indicates that the public show concern and wish care to be taken over the form data sharing takes with private companies and forms of control over use of personal data. This aspect of the public response may interact with policing if private companies have a commercial stake or interest in how police adopt or manage the use of facial data and recognition technology.

2) Can police demonstrate public benefit and assurance of safeguards?

We recommend that:

It is more widely recognised that the practice and principles of policing to reduce crime is a complex process in which there are trade-offs of benefits vs harms, and that there are very different forms that the application of facial recognition technology for policing can take.

For each distinct application of the technology there should be an appropriate form of public engagement, trials and an evidence base.
As next steps, we plan to appoint and consult independent experts on the governance of facial recognition technology and digital recognition technologies, including the frameworks that pertain in Scotland, in the course of our research activities. Look forward to updating this sub-committee in 2020 with the results of our Citizens’ Biometrics Council, a national citizens assembly.

We would be delighted to interact further with this committee to ensure the questions we ask are fully in view of the latest evidence.

3) There is a need to pause and take stock of how facial recognition will be applied, for greater clarity on scenarios and preparation for their adoption into practice.

The 2026 strategy for policing in Scotland includes a hypothetical scenario that includes the use of facial recognition for identifying a suspect, however it offers no further evidence or clarification regarding how the expectation of benefit and safeguards are addressed.

We propose addressing this scenario, and others like it, under the following model framework.

3.1. What is the task?

Facial recognition technology usually refers to using advanced statistical analysis on images of people to do one (or more) of the following tasks:

- **Detection** – identifying that there is a face in an image, and where it is. This is usually the first step of a facial recognition process, to enable matching, identification or classification on only the relevant parts of an image.
- **Matching** – comparing a facial image or images against a pre-existing set of images to see if there’s a match e.g. matching faces from shop surveillance footage against a list of images of barred persons or matching faces from a crowd against images of ‘persons of interest’ in police watchlists.
- **Identification** – comparing a face to a specific identity. This could be done for two purposes:
  - **Verification** – answering the question ‘is this person who we think they are?’, such as the police checking if the person in an image matches their suspect.
  - **Authorisation** – answering the question, ‘Is this person who they claim to be?’, usually to allow access to something, such as using Face ID to unlock an iPhone.
• **Classifying** – identifying a characteristic of a face, such as age, gender or expression e.g. at a supermarket checkout, to assess whether someone is old enough to buy alcohol.

In the case of the intended police use in Scotland, it would seem to rely first upon detection and watch list composition, and subsequently be aimed at matching and identification.

### 3.2. Where does the data enabling facial recognition come from?

Facial recognition systems are biometric systems – they use biometric data, which is sensitive as it’s very personal and based on biological characteristics that are hard for people to change. If someone finds out your password, you can change it. But if someone has a recording or photo of your face, that’s much more difficult. Many people already have plenty of images of their face on the internet, and it can be easy not to notice if you’re recorded by CCTV, which can make it difficult for people to know when their data might be collected or subject to facial recognition technology.

Not all facial data is the same – here are several ways that the data for facial recognition system may differ across systems:

- **Personal/private vs. public** – are images taken from the public domain, in a public place or collected privately?
- **Stored vs. temporary** – will data processed be stored long-term, or is it discarded after processing? If it’s stored, where will it be stored?
- **Static vs. video** – the methods used for facial recognition on static and video images will differ.
- **Resolution and image quality** – resolution and other quality factors such as lighting will make images more or less likely to be accurately recognised by a system.

There are also specific considerations around training data – which is initial data used to develop a machine learning model for facial recognition technology, often referred to as ‘training’ the model. This is typically a set of images or features already labelled by a human that the model can ‘learn’ from.

Additional considerations here include:

- **How representative the images are and the risk of bias** – if one group of people is over/under represented in the training data, the system might be better/worse at recognising them.
- **If we can assume that accuracy issues can be improved upon, what are the standards that would make the use of such a powerful technology proportionate?**

### 3.3. Where and in what way is the technology deployed?
Facial recognition systems can be deployed in different environments or scenarios, such as in airports, bars or out on the streets. Some ways to think about these different deployments are:

- **Live/real-time vs. post-hoc** – whether images are processed ‘live’ (meaning near-real time) versus at a later point, can change the way outputs can be used and could have implication for transparency and civil liberties. For instance, ‘live’ facial recognition technology can result in actions being taken immediately, whereas performing facial recognition on historical images or video, such as CCTV from five years ago, raises questions as to the circumstances in which it is right to perform that analysis and what severity of problem should it solve.

- **Controlled vs. uncontrolled** – a controlled environment is one where important factors like lighting, background and position can be controlled, like in a lab environment, or e-passageport gates where parts of the process are standardised. An uncontrolled environment is the real world, where all these things may vary, making facial recognition much more challenging.

- **Transparency** – those deploying facial recognition technology may be more or less transparent in the fact it is being used, how it is being used and how it works. That means we may not always be able to identify the characteristics for every system.

4. **Conclusion**

The hurdles involved in successful adoption of new technology, and the extent of preparation for ethical facial recognition technology in practice, could be further articulated in the evidence pursued by this inquiry.

There are presently documented shortcomings in the national infrastructure and some defined goals for improvement: example, it is Home Office policy that individuals not convicted of any crime can apply to have their custody image deleted, however this policy has not resulted in full implementation of this principle, meaning that many such persons are included in the database. In the Scottish context, how does Police Scotland ensure that principles apply proportionately? Is the approach to camera surveillance pursued in accordance with the stated policing principles e.g. in a way that is “engaged with local communities”, and is it proportionately pursued to “prevent crime, harm and disorder”?

In our next phases of work we will ask for evidence in detail of the benefits that new adoption of the technology is expected to bring, such as for police forces, and for companies. We will seek to inform guidance with evidence from our public engagement process, and from our associated expert review conclusions about the forms that future governance could take.

Ada Lovelace Institute
1 November 2019

---

### Castle Shopping Centre

This scenario shows how we might respond to a series of shoplifting offences. With easier crime reporting, better evidence gathering and efficient processes, officers have more time to deliver excellent services. The front line is highly connected and informed. There is better information sharing with partners.

1. Series of thefts committed by multiple suspects

3rd of March 2026, a series of thefts were reported in stores in the Castle Shopping Centre, Glasgow. A number of suspects were believed to be involved. The Centre's own security team have been at the scene and have spoken with staff.

2. Crime reported via online self-service portal

A security guard reviews the information gathered. He logs on to the police self-service portal on his smart device. He is able to quickly and easily report the thefts, without needing to call. The security guard adds detail on the location of the thefts, value of goods stolen and an eyewitness account. He securely uploads the evidence such as CCTV footage, editing the file online to focus on the crime's time frame.

3. First point of contact with Police Scotland

Police Scotland staff review and assess the report. The incident is graded according to the prevailing risk and focussed on reducing harm. A risk assessment for this incident identifies there is no immediate threat and an acknowledgment and reference number is sent to the reporter as it is a commercial victim.

4. Facial recognition identifies suspect

A crime and investigation log is automatically populated. Artificial intelligence (AI) scans the footage, identifying a main suspect via facial recognition however images of the accomplices are too blurry. An intelligence file is automatically populated with a suspect profile including associates attached to the log. The AI begins to build an evidence case.

5. Integrated offender and location management

Once the crime and investigation log is created real time information and intelligence is digitally circulated to community police officers and community support officers. The information report highlights Castle Shopping Centre as an emerging ‘hot spot’ and identifies the suspect. Through effective partnership working an alert is also sent to local businesses in the shopping centre and surrounding area.