POLICE USE OF FACIAL RECOGNITION: A GUIDE

Home Office

POLICE USE OF FACIAL RECOGNITION

• A man is spotted in a crowd. He is suspected of being part of an organised crime gang which had stolen jewellery worth over £4 million. He is arrested and charged.

• Police stop a 15-year-old they believe has been reported missing. He refuses to say who he is, so they identify him using an app on their phone and take him to safety.

• A woman reports that a stranger tried to attack her after she got off a bus. The police match CCTV footage of the suspect to his 14-year-old custody photo. Just 48 hours later, he is arrested. He is a known sexual predator and is now in prison for life.

These are just three real-life examples of how, every day, the police use facial recognition to solve crimes and protect vulnerable people.

However, not everyone thinks the police should be using the technology. Civil liberties groups believe that people's privacy is being unjustly invaded. Others are concerned that the technology makes too many mistakes, or that it could be used to unfairly target people from ethnic minority backgrounds.

This guide explains what facial recognition is, how the police use it and the rules and regulations they have to follow when they do.

CONTENTS

LOCATE

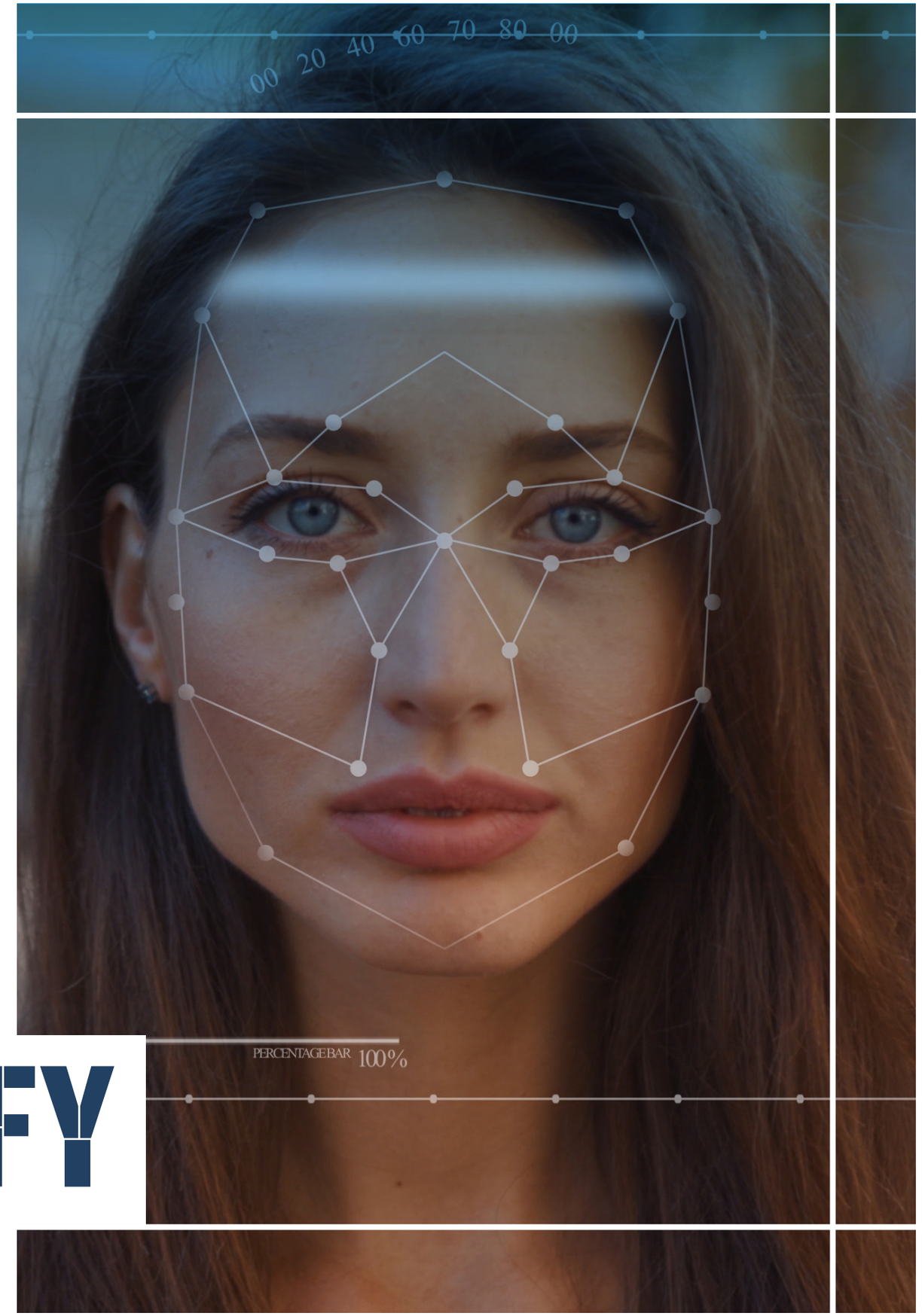
WHAT IS FACIAL RECOGNITION?

Facial recognition technology is used by many people in their daily lives e.g. to unlock smartphones and laptops or to make card payments.

It is also used at the airport by people returning to the UK. The machine uses facial recognition to check that a person matches the photo in their passport.

Facial recognition can also be spotted at some concerts and football matches helping the police to locate known offenders.

IDENTIFY



Facial recognition: Identifying distinctive features

A person's facial features are distinctive. Because of this, scientists have been able to come up with ways to measure and record them in order to help identify people. This is known as biometrics. The most well-known biometric is the fingerprint, which has been used by the police to identify criminals for over one hundred years.

Computers first learnt to recognise faces in the 1960s. Now, a computer can help to correctly identify a face quicker than anyone could. As an example, if a police officer was looking for a suspect, it might take an average of two weeks or more to find them using traditional policing methods. Officers can use facial recognition technology to help them identify or locate that same suspect in a few hours and sometimes within minutes.

How facial recognition technology is used

Facial recognition technology is normally used in one of two ways:

To verify or 'authenticate': A smartphone scans a face and checks it against the image it has.

To help identify or locate: A computer checks an image of a person against a list of known faces and suggests possible matches. This is how the police use facial recognition.

HOW THE POLICE USE FACIAL RECOGNITION

Facial recognition is widely used by the police in England and Wales. Many believe it has huge potential because of how quickly it can help identify suspects or locate those wanted by the police or the courts. It is proving to be a useful way of finding people who are missing or vulnerable or to help identify a person who is found deceased.

All this frees up police time and resources and should, in theory, mean the police are also able to investigate more complicated crimes or spend more time on the beat.

At the moment, the police use three different types of facial recognition. These are:

– Retrospective Facial Recognition
– Operator Initiated Facial Recognition
– Live Facial Recognition

Retrospective Facial Recognition

This is used by all police forces in England and Wales, with thousands of searches being carried out each month. It is used after a crime has taken place to help the police identify suspects quickly, and has been used by the police for many years.

When a crime is reported, the police might gather footage from CCTV cameras, mobile phones, dashcams, doorbells or social media as part of their investigation. If they find a person they want to identify, they send the images to someone who has been trained to use facial recognition.

The images are compared against the Police National Database, a library shared by police forces of the custody photos of known people. The system then produces a list of the most similar images and these images are reviewed by a specially trained operator who decides whether there are any matches. If they think they have a match, they then pass it on to an investigating officer who will do additional checks and follow the usual process for an investigation.

Real life examples

A bus driver is attacked with a knife in Tower Hamlets. The police use facial recognition to identify a suspect, who is arrested and charged with grievous bodily harm with intent. He is later sentenced to five years in prison.

An argument between drivers ends up in a racially aggravated assault. The police use video footage of the attack to identify a suspect.

A victim is sexually assaulted by two strangers they met at a local bar. Footage from a doorbell camera is used to find one of the suspects.

CHECK

Operator-Initiated Facial Recognition

This is used by individual police officers to check the identity of someone they have come into contact with by comparing their photo with a list of known people. If a police officer has a reason to speak with someone who is either unable or unwilling to give their name, they can take their photo and use an app on their phone to find out who they are. The idea is that it helps officers on the beat identify someone without having to take them to a police station.

South Wales Police and Gwent Police are using the technology.

Real life examples

A suspected shoplifter tries to give police officers false contact details. The police use the app to find out who he is and arrest him for theft and obstructing the police.

Police officers get a call to help a drunk man on the street. He cannot speak and does not have any ID on him, so officers use the app to find his name and address before taking him home.

Live Facial Recognition

At least thirteen police forces have used or are using this technology. It helps the police find people who are wanted by them or the courts, when they are in public places. It is known as live facial recognition because it uses live video footage of people passing a camera.

When this type of facial recognition is in use there may be a police van with a camera mounted on top or a camera fixed to a lamppost. There will be lots of police officers about and signs saying something along the lines of, 'Police live facial recognition in operation'. This is because the police have a duty to let the public know that if they walk past their camera their face will be scanned. The police, however, are not looking for just anyone; they have a specific list of people who are wanted by the police or the courts. This is known as a 'watchlist'. The computer checks the faces of passers-by against this watchlist. Anyone not on the watchlist will have their face blurred and their biometric data deleted immediately. If a potential match is found, an alert is sent to the police officer who then compares the two images and decides whether they match. If they do, the police officer will follow the usual process to decide what action should be taken. This might include arresting the person.

Real life examples

A man wanted for domestic grievous bodily harm is arrested after walking past a police facial recognition van. Officers had been looking for him, using traditional search methods, for three weeks.

Over the course of many months, live facial recognition correctly flagged registered sex offenders on the police watchlist. The police stopped each one, check the terms of their conditions and over 100 were arrested for breaching those conditions.

The police put a facial recognition van outside a concert venue, looking for suspects on a watchlist. They find that after the concert they did not get a single report of a mobile phone being stolen. The average number of thefts the police would normally expect at such a concert is around 220. They arrested one person for going equipped to steal after he was found carrying a tool used to remove SIM cards.

CONCERNS ABOUT POLICE USE OF FACIAL RECOGNITION

Concerns have been raised about the police's use of facial recognition and, in particular, the way they use live facial recognition. Civil liberties groups believe it unjustly invades people's privacy – that innocent people should not have to have their faces scanned.

They and others also believe that live facial recognition makes too many mistakes. And because at some settings some versions of the technology are more likely to wrongly identify someone who is Black, Asian or female than someone who is White or male. They are also concerned that the police will not use it fairly.

The next section sets out in detail the work that has been done so far to address these concerns. It covers the laws and guidance in place to ensure the police use facial recognition fairly and responsibly. It sets out how facial recognition technology is tested for accuracy and bias, and what independent testers found when they assessed facial recognition technology used by the police.

THE LEGAL FRAMEWORK:

Ensuring the police use facial recognition fairly and responsibly

There are laws and guidelines in place for the police to follow when they use any type of facial recognition technology.

For example, for live facial recognition, the police use their common law powers, which were created by the courts. To create a watchlist, they use the powers given to them by Parliament, which allows photos they hold to be used for a valid policing reason. There are four other laws created by Parliament, which the police must be able to show they have followed when they decide to send out a facial recognition van. The laws are there to protect people's data, human and equality rights.

To help the police follow the correct procedure, there is the College of Policing's Authorised Professional Practice (APP) guidance. There is also guidance from other organisations and each force will have its own published policy documents as well.

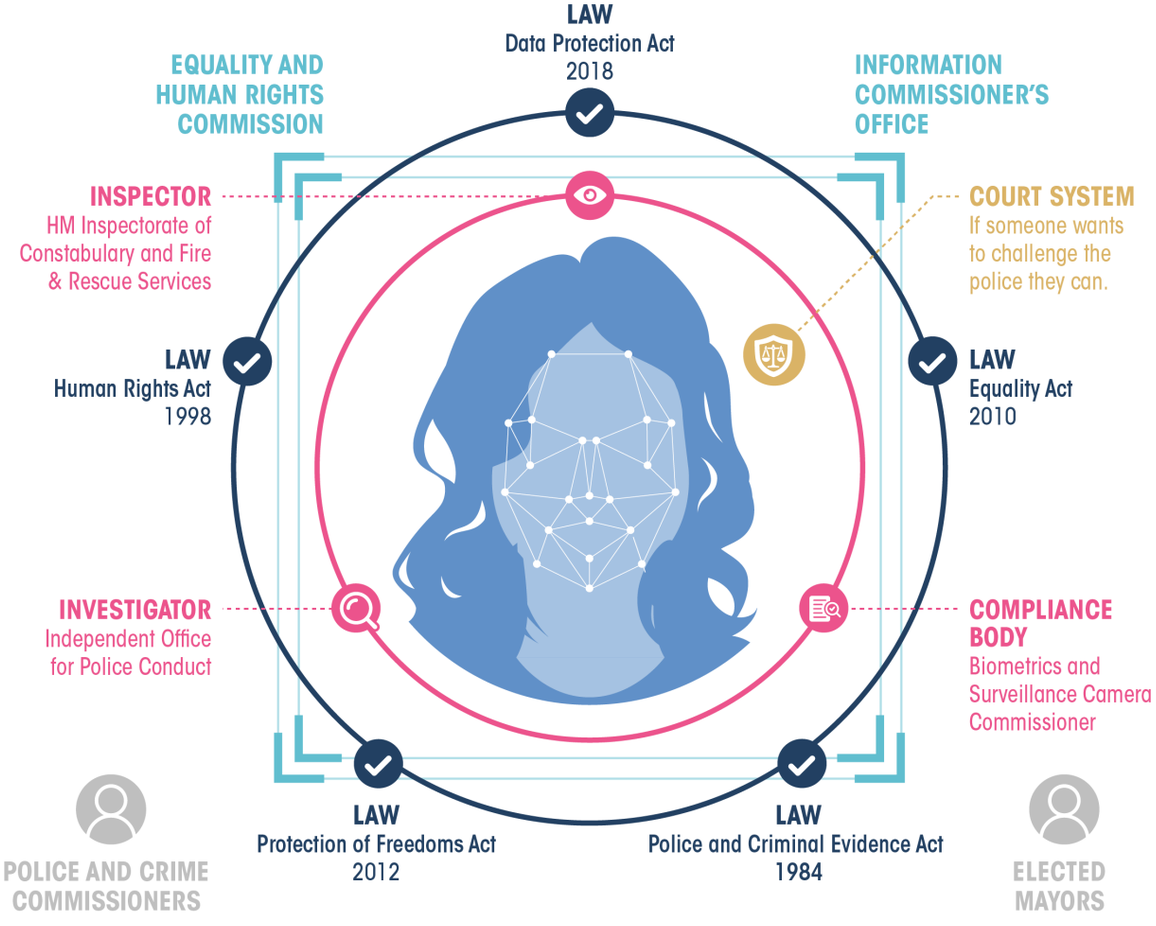
To use retrospective and operator-initiated facial recognition technology, the police also need to follow the laws and guidance in place.

There are two regulatory bodies which keep an eye on what the police are doing. There are another three public bodies which are there to inspect, investigate and make sure they comply with the law and guidelines. And, finally, there is the court system, where if someone wants to challenge the police they can.

Legal framework

COMMON LAW POWERS | LAWS BY PARLIAMENT | REGULATORS | OVERSIGHT BODIES | COURTS

CODES OF PRACTICE & GUIDANCE — College of Policing APP for live facial recognition | Surveillance Camera Code | ICO video surveillance guide ▸ **POLICE POLICY DOCUMENTS**



That is the legal framework for facial recognition. Here is an example of what it would look like in practice:

Police officers decide they want to use live facial recognition.

They must be able to show that there are valid policing reasons and why facial recognition is the right tool to use. They also have to set out where and when they plan to use it.

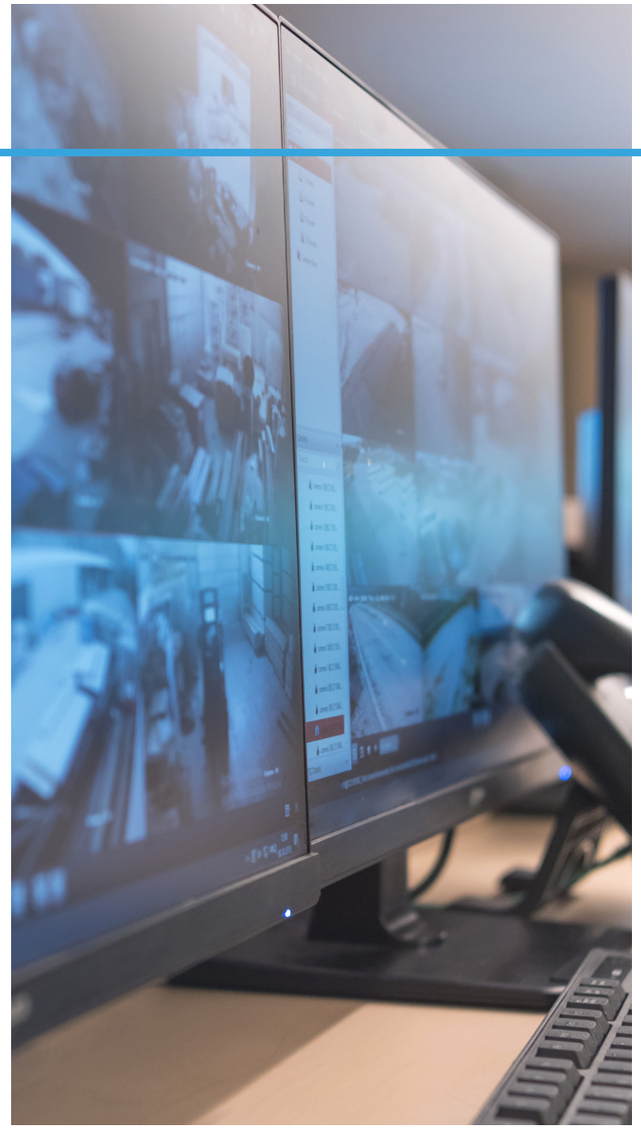
They create a 'watchlist' for that operation. This is a list of people the police want to find. For example, they might be suspected of committing a crime or they could have been registered as missing or vulnerable.

The police must make the public aware that they are using live facial recognition. This might include using social media and placing bright signs on lampposts to let the public know they are about to enter an area where their face will be scanned.

When the operation is running, the vast majority of people who walk past the camera will not match any of the images on the watchlist. These people's biometric data is immediately and automatically deleted.

If the system flags someone it thinks is on the watchlist, the system will send the still CCTV image and the watchlist image to police officers on the ground. The police officers decide whether it is a match and whether to then approach that person. The police never rely solely on a machine – a trained police officer will always check what the system has found. This safeguard makes it far less likely that the police will arrest the wrong person.

If the police believe the system has found a person on their watchlist, they approach that person and talk to them as they would anyone else they wish to speak with. The watchlist is deleted when the operation is over.



TESTING LIVE FACIAL RECOGNITION FOR ACCURACY

There are lots of different facial recognition algorithms in use today, all developed by different companies. Some are more accurate than others.

How accuracy in live facial recognition is measured

When testers check how accurate a live facial recognition algorithm is, they are looking for how often it correctly puts people into four different groups. These groups are:

1. People who are not wanted and therefore not on a watchlist. This is the vast majority of people who walk past a live facial recognition camera. They are known as **true negatives.**

2. People who are wanted and on a watchlist are **true positives.**

3. People incorrectly identified as being on a watchlist are **false positives.**

4. People who are wanted, but the algorithm does not recognise them are **false negatives.**

The most important thing for accuracy is that the technology itself is good – that it can still get results with grainy or blurry images, for example. But the other thing that is important is the threshold the system is set at. The threshold is the setting which decides how similar two faces need to be for the computer to flag a possible match.

A higher setting will mean the computer needs to find more similarities between two faces. A lower setting means the opposite – there can be fewer similarities and the system will still flag a match.

Using a lower setting: This will throw up more potential matches. However, it is also more likely to wrongly identify people as being on a watchlist.

Using a higher setting: The computer will not find as many matches. This means fewer people will be wrongly identified. However, it is more likely to miss people who are on a watchlist – and let wanted people walk past unnoticed.

The threshold a system is set at makes a big difference to how good a system is at putting people in the right group. It is the users of the system, in this case the police, who have to decide what balance they think is right according to operational circumstances. The police must take into account their duty to treat everyone fairly and equally when they do this.

Bias

Facial recognition relies on artificial intelligence (AI), which involves teaching the system to recognise faces. An AI system is only as good as the data that is used to teach it. With facial recognition, this means the images the developers have fed it so that it learns to identify faces. So, for example, if the AI is not shown enough pictures of Black people then it may incorrectly identify them more often, because it does not have enough data to go on.

The performance of a facial recognition system can also be impacted by other factors e.g. lighting, which need to be taken into account.

INDEPENDENT TESTING RESULTS

In 2023, the National Physical Laboratory – an independent testing laboratory – looked into the accuracy of the live facial recognition algorithm being used by South Wales Police and the Metropolitan Police. This included looking at the threshold settings each used. The scientists were particularly interested in finding out if there was any difference in accuracy based on a person's age, gender or ethnicity.

The testers found there are settings where there was no statistically significant difference in how well the algorithm identifies people according to their age, gender or ethnicity.

They also found there was almost a nine in ten (89%) chance that the algorithm would correctly identify someone on a watchlist. When it came to incorrectly identifying a person who was not on a watchlist, there was at worst a 1 in 6,000 chance that the algorithm would do this on a watchlist with 10,000 images.

These are the settings both South Wales Police and the Metropolitan Police use. However, the report noted that if the police changed their settings, the algorithm would become less accurate.

The 10 live facial recognition vans rolled out in August 2025 have the same algorithm used by South Wales Police and the Metropolitan Police.

The scientists have also tested the retrospective facial recognition algorithm used to conduct facial image searches on the Police National Database. They found that in a limited set of circumstances the algorithm was more likely to incorrectly include some demographic groups in its search results. They also found that if a correct match was in the database, the algorithm found it in 99% of searches, at the settings used by the police.

As mentioned earlier, a specially trained operator visually assesses the returned images and decides whether there is a match. An investigating officer also does the same and considers all the available evidence. This reduces the risk of images incorrectly returned by the algorithm informing police decisions. Established training, guidance and police practices have been reissued and promoted to all trained users reminding them of the long-standing manual safeguards in place, to make sure the algorithm does not solely influence investigations and decisions.

The scientists also tested a new national retrospective facial recognition algorithm. The testing found there are settings which can be used where there are no statistically significant difference in how well the algorithm identified people according to their age, race or gender. The new algorithm will be trialled with the police in early 2026 and then evaluated.

FURTHER INFORMATION

More information about how the police are using facial recognition, what is being done to make sure they do so fairly and responsibly and the results from independent testing can be found using the following links:

Police use of Facial Recognition Factsheet
https://www.gov.uk/government/publications/police-use-of-facial-recognition

National Physical Laboratory testing of the Live Facial Recognition technology used by South Wales Police and Metropolitan Police
https://science.police.uk/delivery/resources/operational-testing-of-facial-recognition-technology/

National Physical Laboratory testing of Retrospective Facial Recognition (RFR) algorithm on Police National Database and new national RFR algorithm
https://www.gov.uk/government/publications/facial-recognition-technology-tests-national-physical-laboratory

College of Policing's Authorised Professional Practice guidance for Live Facial Recognition
https://www.college.police.uk/app/live-facial-recognition

Metropolitan Police's facial recognition page
https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/

South Wales Police's facial recognition page
https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/

The Information Commissioner's Office: CCTV and video surveillance guidance
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services
https://hmicfrs.justiceinspectorates.gov.uk/

Equality and Human Rights Commission
https://www.equalityhumanrights.com/

Independent Office for Police Conduct
https://www.policeconduct.gov.uk/

Surveillance Camera Code of Practice
https://www.gov.uk/government/publications/update-to-surveillance-camera-code/

This guide was produced in collaboration with the Accelerated Capability Environment