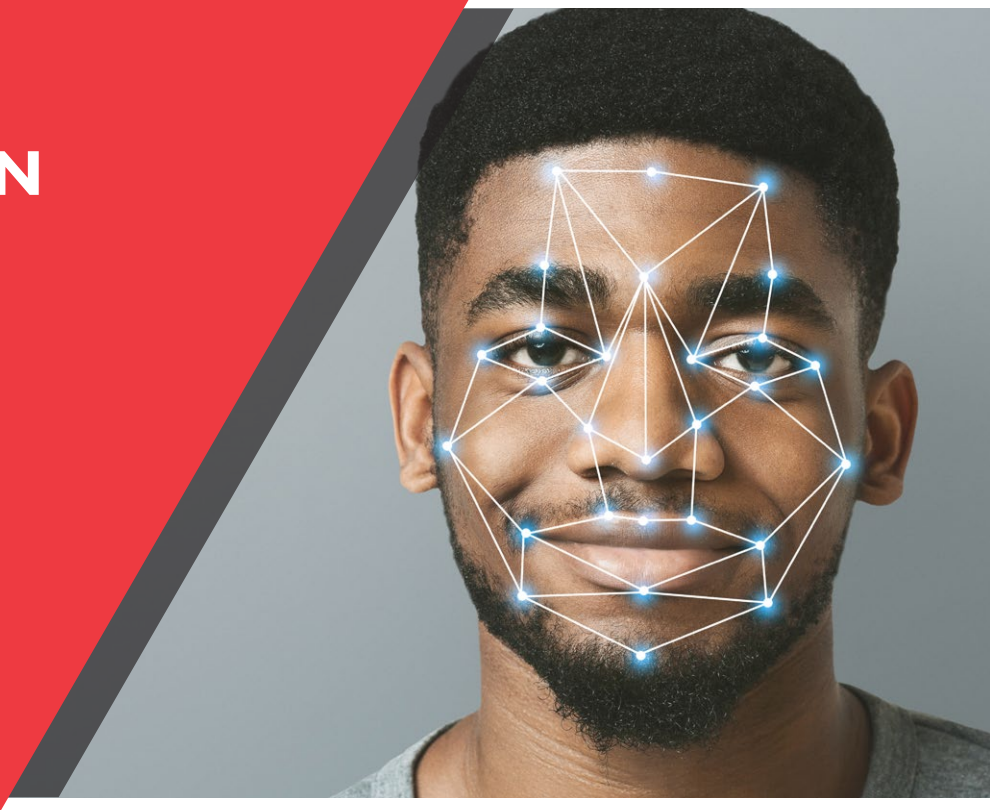
# FACIAL RECOGNITION

An Introduction



Facial recognition is being increasingly used by a variety of sectors to quickly identify people of interest in a large stock of video, or to actively identify and track people in real time.

## What is Facial Recognition?

Facial recognition is a category of biometric security. Other forms of biometric software include voice recognition, fingerprint and palm recognition, and eye retina or iris recognition. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use.

## How Does Facial Recognition Work?

Facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts.

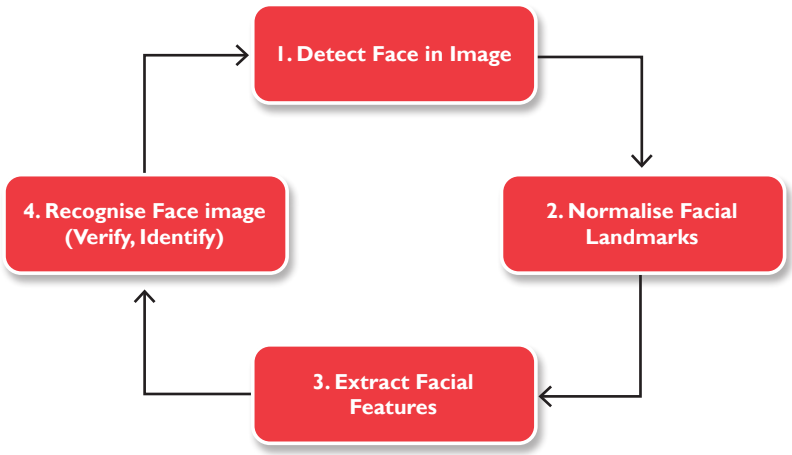
Facial technology systems can vary, but in general, they tend to operate as follows:

## Step 1: Face detection

The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

## Step 2: Face analysis

Next, an image of the face is captured and analyzed. Most facial recognition technology relies on 2D rather than 3D images because it can more conveniently match a 2D image with public photos or those in a database. The software reads the geometry of your face. Key factors include the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.




## Step 3: Converting the image to data

The face capture process transforms analog information (a face) into a set of digital information (data) based on the person's facial features. Your face's analysis is essentially turned into a mathematical formula. The numerical code is called a faceprint. In the same way that thumbprints are unique, each person has their own faceprint.

## Step 4: Finding a match

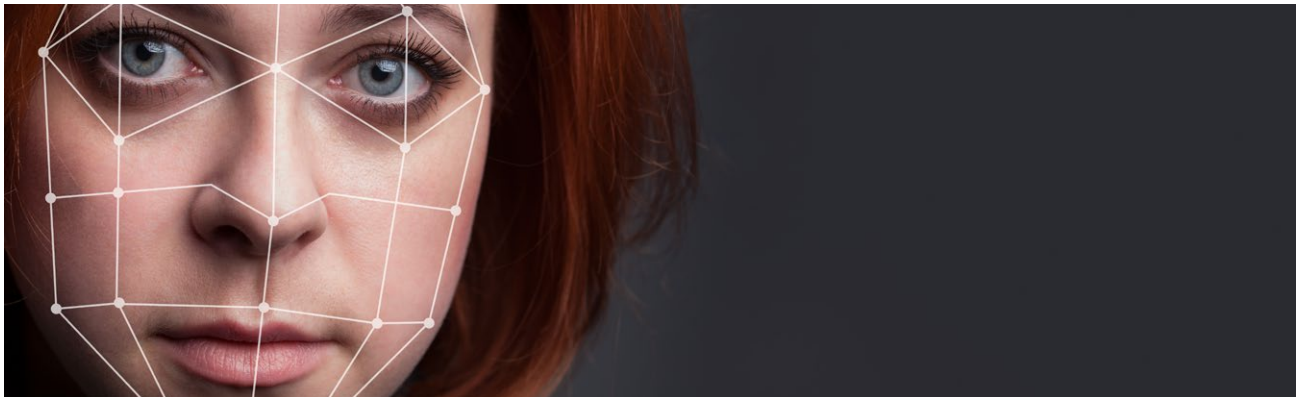
Your faceprint is then compared against a database of other known faces. For example, the FBI has access to up to 650 million photos, drawn from various state databases. On Facebook, any photo tagged with a person's name becomes a part of Facebook's database, which may also be used for facial recognition. If your faceprint matches an image in a facial recognition database, then a determination is made.

Of all the biometric measurements, facial recognition is considered the most natural. Intuitively, this makes sense, since we typically recognize ourselves and others by looking at faces, rather than thumbprints and irises. It is estimated that over half of the world's population is touched by facial recognition technology regularly.

## Why are Biometrics Used in Security Systems?

Traditional access systems have a critical vulnerability: credentials and data can be shared or stolen, allowing someone other than the intended user to access the facility. Biometrics, however, do not have this vulnerability. Because everyone has a unique biometric code that is always with them, it is very difficult for anyone other than that person to access it.

This is why, while not all biometrics are equal in terms of security, even some of the least secure biometric systems are still more secure than traditional security systems.



# What are the Benefits of Facial Recognition?

The main benefits of using biometrics are security, convenience, reduced crime, reduced bias and reduced costs.

## Security

**Unique To User:** As biometrics are unique to a person's biology, it is extremely difficult for their identity to be taken or used by anyone other than the intended user.

**Difficult to duplicate:** Traditional access tokens such as keycards can be easily duplicated using a simple keycard duplicator, illustrating the security vulnerabilities of legacy access control credentials. Biometrics, however, are generally much harder to copy because most modern biometric systems use liveness tests to ensure that the biometric data is coming from an actual human and not a forged replica.

## Convenience

**Cannot be lost or forgotten:** Biometric access control systems are remarkably convenient as they allow authorized users to access a facility without needing anything other than themselves.

**Easy access:** Your biometric ID is always at hand, so no more fumbling in your pocket for a fob or ID card. Your hand, finger, face or eye is your ID.

**Efficiency:** Most biometrics are able to identify users in under a second, eliminating the inefficiency and time delays caused by manual identity checks, passwords, or PINs.

## Reduced Crime

Face recognition makes it easier to track down burglars, thieves, and trespassers. The simple knowledge that a face recognition system is present can serve as a deterrent, especially to petty crime. Aside from physical security, there are benefits to cybersecurity as well. Companies can use face recognition technology as a substitute for passwords to access computers. In theory, the technology cannot be hacked as there is nothing to steal or change, as is the case with a password.

## Removing Bias From Stop And Search

Public concern over unjustified stops and searches is a source of controversy for the police — facial recognition technology could improve the process. By singling out suspects among crowds through an automated rather than human process, face recognition technology could help reduce potential bias and decrease stops and searches on law-abiding citizens.

## Reduced Costs

**Fewer Security Staff:** Biometric access control systems can save companies money by reducing the need for dedicated security staff at main access points.

**Zero Replacement Costs:** Access control systems that use physical tokens such as keycards and fobs incur an extra hidden cost: lost token replacement rate. Lost cards and fobs are an all-too-common occurrence.

**Protect Expensive Equipment:** The cost of potential security breaches can be extremely expensive. In manufacturing facilities, for example, the use of machinery by unauthorized persons can void the warranty of the machine, creating enormous out-of-pocket costs to repair if it breaks, not to mention the cost of any injuries.

**Integration With Other Technologies:** Most facial recognition solutions are compatible with most security software. In fact, it is easily integrated. This limits the amount of additional investment required to implement it.

## Potential Future Applications

As the technology becomes more widespread, customers will be able to pay in stores using their face, rather than pulling out their credit cards or cash. This could save time in checkout lines. Since there is no contact required for facial recognition as there is with fingerprinting or other security measures – useful in the post-COVID world – facial recognition offers a quick, automatic, and seamless verification experience.

# What Are The Downsides Of Facial Recognition?

## Surveillance

Some worry that the use of facial recognition along with video cameras, artificial intelligence, and data analytics creates the potential for mass surveillance, which could restrict individual freedom. While facial recognition technology allows governments to track down criminals, it could also allow them to track down ordinary and innocent people at any time.

## Scope For Error

Facial recognition data is not free from error, which could lead to people being implicated for crimes they have not committed. For example, a slight change in camera angle or a change in appearance, such as a new hairstyle, could lead to error.

## Breach Of Privacy

The question of ethics and privacy is the most contentious one. Governments have been known to store several citizens' pictures without their consent. In 2020, the European Commission said it was considering a ban on facial recognition technology in public spaces for up to five years, to allow time to work out a regulatory framework to prevent privacy and ethical abuses.

## Massive Data Storage

Facial recognition software relies on machine learning technology, which requires massive data sets to "learn" to deliver accurate results. Such large data sets require robust data storage. Small and medium-sized companies may not have sufficient resources to store the required data.

# So is Facial Recognition Right for You?

Whether facial recognition is right for you to help boost your security, as well as minimising viral transmission, is a question of deciding whether the benefits outweigh the downsides.

If you are not sure, please contact us as we are here to help. We can provide a structured approach to understanding your threats and vulnerabilities, which can then be used to provide an objective view as to whether facial recognition would overall improve your security system.

## If you would like to find out more please contact us:


UK: 08459 000 447 (option 1)

enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447

g4ssales@ie.g4s.com