Nirovision

Free Guide

The ultimate guide to facial recognition

Everything you need to know about how facial recognition works, its use cases, biggest myths and more.

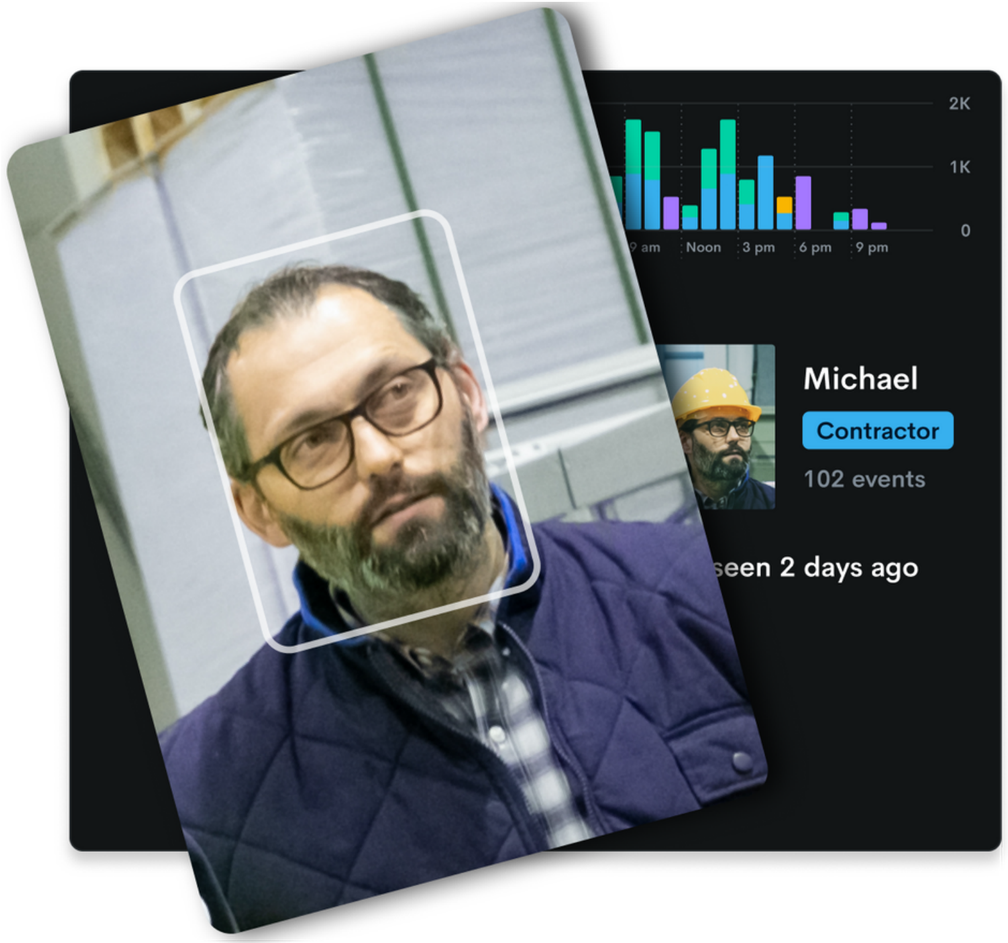


Table of Contents

Introduction

From banking and payment, to recording who enters the workplace, we're increasingly using facial recognition to make life easier, safer and more secure.

As the technology continues to evolve and more devices and software start leveraging the benefits of facial recognition, it's going to become a part of everyday life, if it's no already. So to make sure you're up to speed and ready for what's to come, here is our guide to facial recognition and how it can potentially benefit your workplace.

> *The facial recognition market was valued at USD 4.84 billion in 2020, and it is projected to be valued at USD 12.75 billion by 2026, registering a CAGR of 17.6% over the forecast period from 2021 to 2026 - Mordor Intelligence*

5 frequently asked questions about facial recognition

What is facial recognition?

Facial recognition is a technology that can match a human face from a digital image or a video frame against a database of faces usually for ID verification purposes. Categorised as biometrics due to the measurement of a human's physiological characteristics, facial recognition is being widely adopted in smartphones and workplaces due to its security and the fact it is touchless.

How accurate is facial recognition?

There's no easy way to answer this as there are various types of facial recognition technology being used across a multitude of industries and for many different applications. In general, the accuracy of facial recognition is as only good as the quality of faces in a database.

Who are the biggest users?

The biggest users are everyday consumers thanks to smartphones using facial ID to enable touchless payments, more secure log into platforms and services, and access to your phone simply by looking at it. According to research, the future growth of facial recognition will be driven by governments, law enforcement, automotive and specific industries for security and access control.

What are the disadvantages?

While accuracy of facial recognition has greatly improved over time there can still be challenges due to low light, bad camera angles, and direct sunlight making it hard to match a face. There are also privacy concerns around the use of facial recognition by government and law enforcement.

What are the benefits of facial recognition?

Facial recognition greatly strengthens security measures. Unlike swipe cards and pin codes that are easily shared, face identification requires a person to be present to verify their identity. It also provides a touchless way to make payments, open doors automatically, and check in to the workplace.

How does facial recognition work?

Face recognition technology uses computer algorithms to identify a series of numerical vectors that represent key features detected in the image of a face. This can includes things like the distance between the eyes or shape of the mouth. This data which we call embeddings, is compared to other images in your facial recognition database in order to find a match.

It's important to note that embeddings are generated from the image of a face, but an image of a face cannot be generated from an embedding.

If there is no match then your face is classified as unknown and ignored. So if you haven’t opted in or been added to a particular facial recognition database then you cannot be identified.

Often the verdict of a match relies on thresholds which are configurable. For example, if using facial recognition for access control, you may want to only confirm a match if the algorithm is 90% confident compared to another use case where a 75% match will suffice.

The use cases for facial recognition

- Record who enters the workplace
- Facilitate secure transactions
- Recognise those on a watchlist
- Grant or deny access to doors
- Track time and attendance
- Identify and tag people in photos
- Verify people for border control
- Find missing persons
- Provide touchless payment
- Provide creative filters for social media use
- Unlock smartphones
- Provide smarter digital billboard advertising
- Support self exclusion at casinos

Is facial recognition secure?

The idea of being identified by facial recognition software can make some people feel uneasy, because a face is very personal to an individual. Yet facial recognition is very secure and a lot more private than other platforms like social media where we freely upload all sorts of photos and sensitive information.

Any cloud technology can be vulnerable to attacks but that doesn't stop us from banking online, or sending important files by email. Why? Because we are confident that security measures that software providers put in place will protect us against hackers and cyber attacks. Facial recognition platforms are similar in that security protocols are followed to encrypt and protect information, but just like online banking and email, there is some responsibility on users to control what security and privacy procedures are implemented to protect their information.

Here at Nirovision, we take every measure to protect biometric data. Each time you create or update an identity, Nirovision extracts its facial features and generates a fingerprint as a random alphanumeric string of code. This anonymizes the facial data therein, the fingerprint cannot be reverse engineered back into a photo. When you compare faces and identities in our system, you are actually comparing fingerprints.

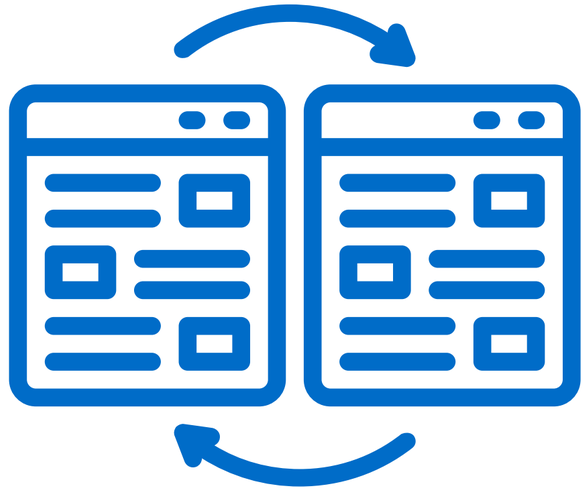
Identities also don’t require a name to be stored in our system, so you can use any naming convention of your choice, along with custom metadata as you require. In addition, faces not recognised are deleted after a certain time and we will not sell your data nor send to any third-party company without your explicit consent.

Facial recognition myths

Myth #1: All facial recognition systems are linked

One of the biggest myths about facial recognition is that all systems are linked. Put another way, if you're identified on one system, you will be identified on other facial recognition systems.

Firstly, there are many facial recognition solutions, using very different technology stacks that simply cannot (or don't want to) link with each other. Take for example the facial recognition on your phone that allows contactless payments. The technology that performs this task, has no interest or connection with the technology that is used to tag friends in photos on social media.



Even if two facial recognition solutions are solving the same problem such as identifying people entering a workplace, that doesn't mean the two technologies share databases. That would be like two competing CRM's linking with each to cross share private customer data. This would be a huge breach of privacy and doesn't make any commercial sense.

If a workplace wants to use the same facial recognition technology across multiple sites to know when a contractor visits one site versus another, then that's possible with a solution such as Nirovision. This however is very different to two separate business entities sharing a database.

In summary, facial recognition software is no different to other software that stores employee or customer data. There are privacy protocols to follow. Plus each software is different and there is no incentive to share data with other businesses.

Myth #2: Facial recognition can identify anyone

If you understand how facial recognition works then you'll understand why this myth is false.

Facial recognition works by looking for a 'match' against a database. If there is no match then your face is classified as unknown and ignored. So if you haven't opted in or been added to a particular facial recognition database then you cannot be identified.

It's important to add that a face only becomes valuable when you can tie information to that face such as a name, a label, a phone number and other metadata. So for a facial recognition system to identify anyone, it would need access to a centralised database with everyone's head shot and vital details.

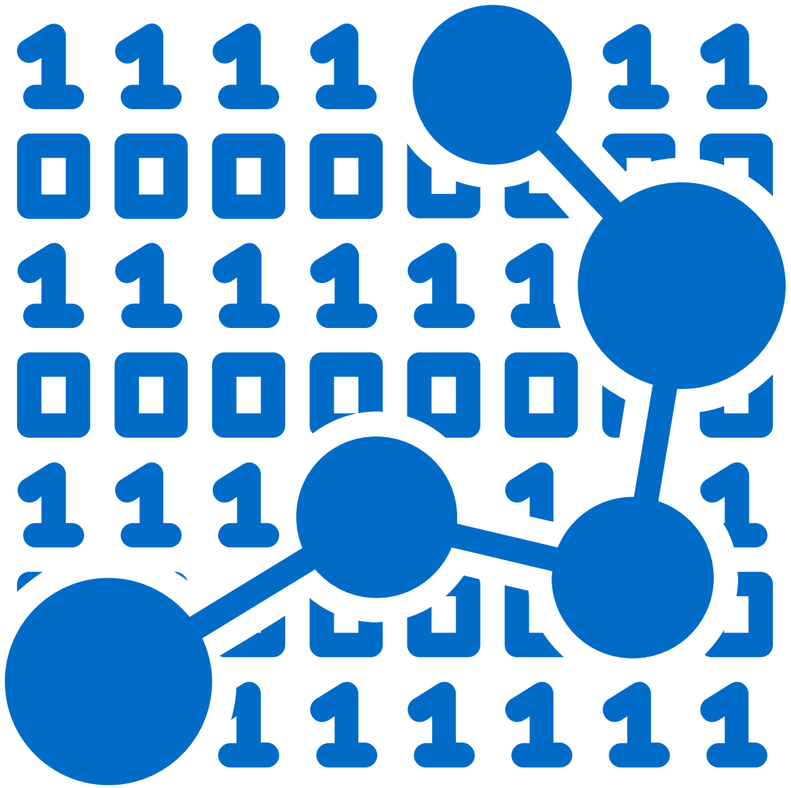
In some cases, a facial recognition system might remember an unknown face (if it sees that face a few times) but remember, a face is as only good as the information associated with it.

Myth #3: A face can be re-created from data points

What if someone hacks a database that I know I am a part of (like my work's HR system)? What if someone steals the server that holds the database? What if someone hacks the cloud provider we use? These are all common fears when it comes to the security of data and the same is true for facial recognition data.

Broadly speaking, data points is what makes up a facial recognition database. Here at Nirovision (and this is the same for most facial recognition software), each time you select a face to create or update an identity, our software extracts its facial features and generates a fingerprint as a random alphanumeric string of code. This anonymizes the facial data therein so the fingerprint cannot be reverse engineered back into a photo.

Accessing a facial recognition user interface is more problematic for privacy and this is why password encryption and who you authorise to have access matters. At Nirovision, we leverage world-class partners that meet the strictest compliance standards to help you protect your data. Our authentication partner is Auth0, an industry leading identity management platform and our cloud infrastructure provider is AWS, with all data being stored and transmitted solely in Australia. Read more about our security and privacy here.



Myth #4: Faces end up on a government database

Faces do not randomly end up on a government database unless a government owned agency is using facial recognition for the purpose of border control, passport or driver license verification. In these circumstances, your data can only be used for a sole task and there are privacy policies around the use of your data. For example, the Roads & Traffic Authority state that “Your photo is protected by the Privacy and Personal Information Protection Act 1998 and can only be used for a driver licence or photo card product.”

In addition, facial recognition data is not easily hacked, intercepted or shared. This is due to the way face recognition data is processed as we learned in the previous myth. This makes it hard for someone to share a database of faces with anyone including the government.

Myth #5: Facial recognition is more reliable than other forms of identification

While facial recognition is a strong form of identification, that doesn't mean the technology on its own is perfect. The same can be said for most forms of identification. For example:

- Driver licences can be frauded
- Pin numbers can be shared with others
- Social media profiles can be made up
- Phone numbers can be ported
- Passwords can be hacked
- Swipecards can be shared

The biggest challenge for facial recognition as a form of identification is accuracy. That's why here at Nirovision our software allows uses to add multiple photos to someone's profile to strengthen their identity.

While accuracy can be a challenge, the technology has a lot of advantages over other methods of identification because biometrics require the person to be present to verify their identity. This is not the case for things like pin numbers and passwords.

Facial recognition technology becomes even more powerful when you combine it with other forms of identification. For example, combining facial recognition with a formal induction process is a powerful way to ensure only those pre-approved can access a work site.

Ensuring people are, who they say they are, is the goal of any identification system. Facial recognition paired alongside other identification methods, goes a long way to achieving this.

Myth #6: Facial recognition stops working as a person ages and their features change

While a person's facial features can change slightly over time, this is generally not an issue for facial recognition systems due to the regularity of the person being identified. As time goes on any changes are noted and updated.

This is no different to how humans remember faces. We find it easy to recognise the people we see regularly, however it's much more difficult to remember someone we haven't seen in 10 years. Facial recognition works in a similar way.

It's also true that the more images of a face, the better the recognition. For example, you've probably seen your best friend in all sorts of guises and situations so your brain has a strong depository of images to make recognising your friend easy. This is the same for face recognition.

Even if someone makes a really drastic change to their appearance such as a male shaving off a beard, a face recognition system may still recognise that person assuming their identity within the system is very strong. The more images, facial expressions and angles of a face, the better the recognition. This is why the facial recognition on your smartphone works so well even if you have your sleep face on in a dark room.

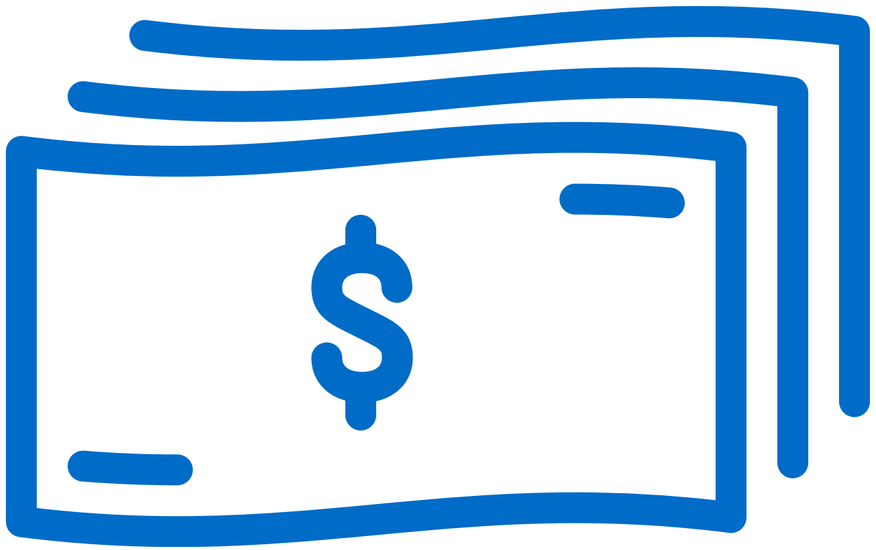
Myth #7: Facial recognition doesn’t work on people wearing face masks

This myth is an extension of the myth that facial recognition doesn’t work full stop. This is not true but accuracy can vary depending on image quality, which brings us to face masks.

Some facial recognition software may still be able to recognise a face even if that face is covered by a mask. This is not always the case but if an identity in a facial recognition database is strong and the facial features unique enough, then it’s possible. We’ve seen it firsthand here at Nirovision (not that we encourage the use of face masks for accurate detection).

As we discussed in the previous myth, the ability for a facial recognition system to identify someone greatly improves when a system can access multiple faces of that person for comparison. If someone starts wearing a mask, you can add images of that person wearing a mask which in turn can help recognition of that person.

All this said, if you want accurate facial recognition then mask wearing is not advised.



Myth #8: Facial recognition is really expensive

There is a perception that facial recognition technology is really expensive but it really depends on the use case. For example, the face recognition you use to log into your smartphone is basically free, whereas implementing facial recognition on hundreds of cameras at an airport may cost thousands of dollars.

In addition to the software, there can be hardware costs such as cameras (in order to capture footage), server (if processing facial recognition on-site), cloud costs (if processing facial recognition in the cloud), and the installation of the hardware.

A workplace wanting to implement facial recognition is very affordable – or at least more affordable than you may think.

If you're interested in what facial recognition costs for your workplace, you can request a quote here.

What are the privacy laws around facial recognition?

The laws around the use of facial recognition vary from country to country. Here in Australia, the Privacy Act states that an organisation must only collect sensitive information about an individual if:

- the individual consents to the collection; and
- the information is reasonably necessary for the organisation's functions or activities

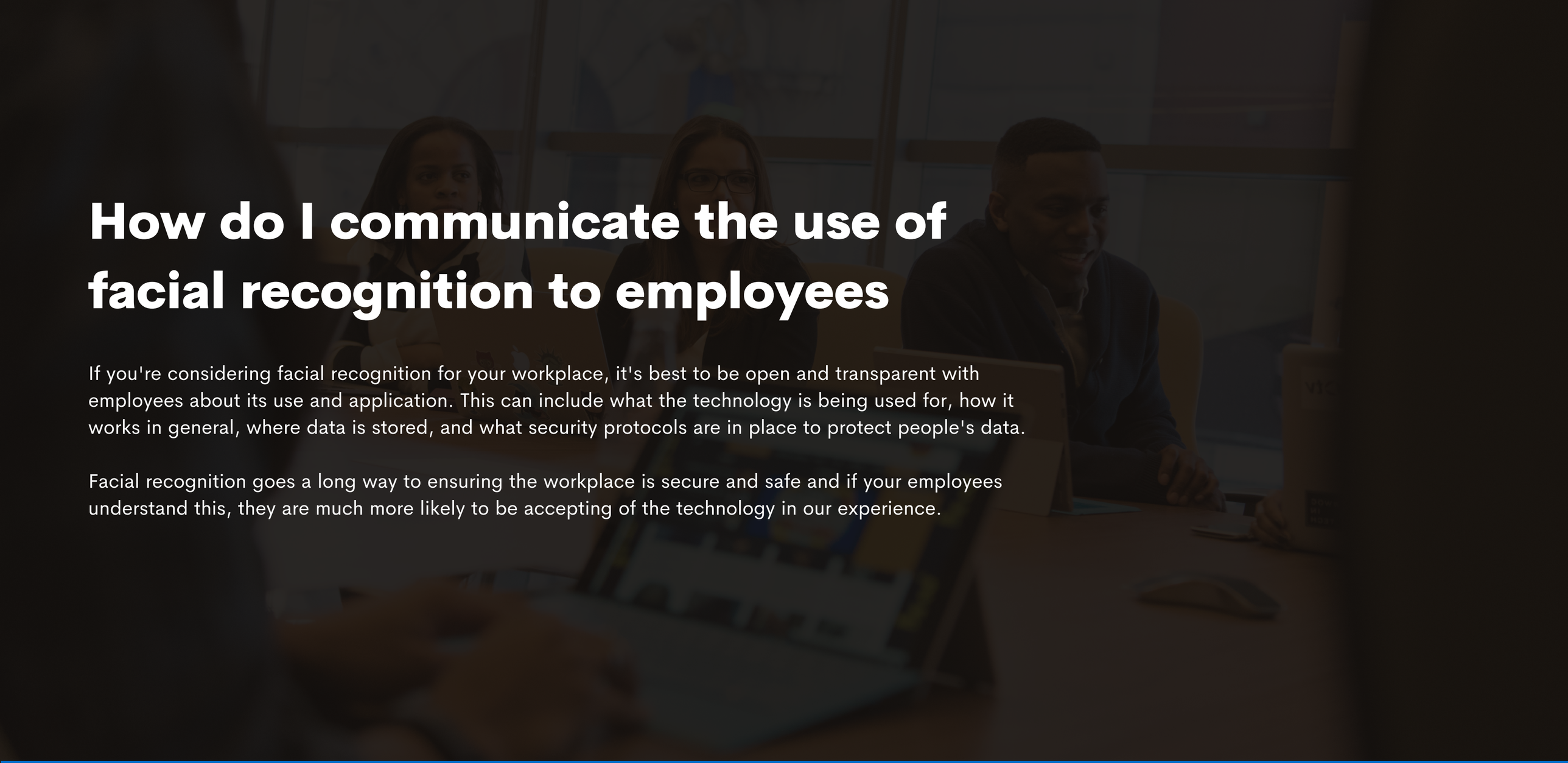
In Australia, the definition of 'sensitive information' has been expanded to include biometric information that is to be used for the purpose of automated biometric verification or biometric identification or 'biometric templates'. Biometric information is 'sensitive information' under the Privacy Act.

An individual can consent to the collection of information via employment agreements, employment onboarding, or at the point of check in.

Organisations should ensure that they tailor their privacy statements and consents to reflect the privacy requirements and obligations of the organisation and the way it collects and actually uses personal information.

To learn more about Australian privacy laws around facial recognition, we commissioned expert lawyer Shah Rusiti, Partner at Teece Hodgson & Ward, to develop the following guide.

Access the guide here.



How do I communicate the use of facial recognition to employees

If you're considering facial recognition for your workplace, it's best to be open and transparent with employees about its use and application. This can include what the technology is being used for, how it works in general, where data is stored, and what security protocols are in place to protect people's data.

Facial recognition goes a long way to ensuring the workplace is secure and safe and if your employees understand this, they are much more likely to be accepting of the technology in our experience.

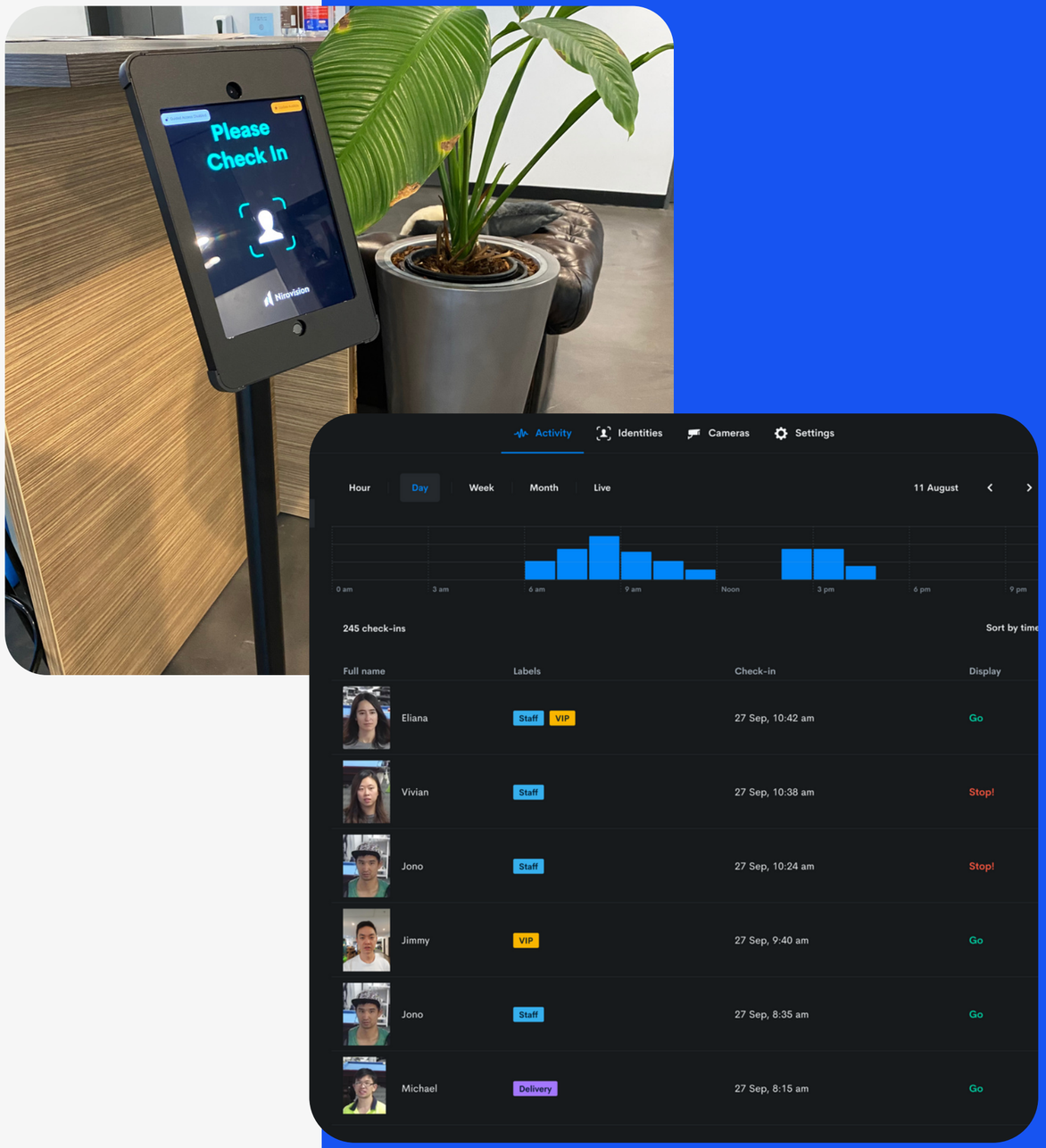
What is the best facial recognition for workplaces?

The best solution depends on your needs. The main use cases for facial recognition in the workplace are:

- Visitor management to check in workers and visitors
- Tracking of time and attendance
- Access control to grant or deny access to doors
- Contact tracing
- Watchlist alarms and notifications for certain people or groups of people
- General insights into how people move around the business, space utilisation

Nirovision facial recognition software helps with all of this, and integrates with VMS, workforce management and access control systems to help make workplaces safer and more secure.

[You can book a demo here to learn more.]



Nirovision

About us

AUSTRALIAN MADE

Headquartered in Sydney, Australia, Nirovision is an Australian owned and developed visitor management solution that uses facial recognition to provide touchless check-ins, temperature analytics and visual contact tracing, along with a host of smart integrations.

Built for industrial businesses, Nirovision is able to identify individuals and their attributes, such as body temperature in real-time. Our software can be set up on an iPad at the entrance for a simpler, safer and more secure check-in process and/or integrated with strategically placed cameras around the workplace to provide visual contact tracing and other workplace insights.

Nirovision.com