Facial Recognition Technology for the Security Industry
How to get it right

ROB WATTS
CEO, CORSIGHT AI

It is not uncommon to see controversial headlines around the use of Facial Recognition within Australia and across the rest of the world. Discussions about this powerful technology can often be dominated by concerns around privacy or ethics, due to disreputable companies who neglect essential ethical practices and ignore critical regulation.

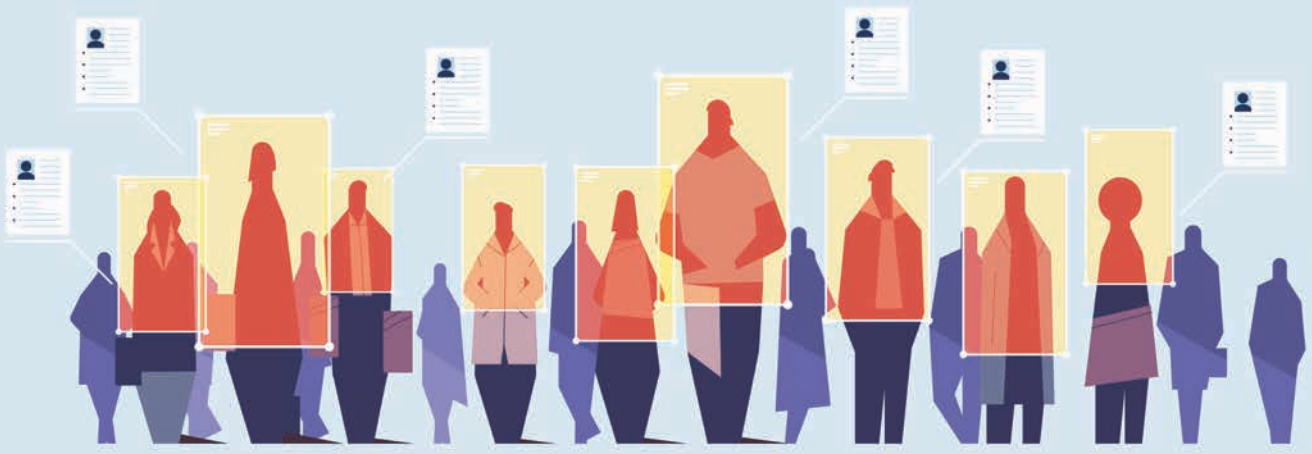
Yet while there is certainly misuse in the industry, there is also huge opportunity if these systems are used as a force for good to protect society and if they are only ever implemented within a framework that prioritises the privacy, safety and equality of all those that encounter it. This is not only possible in the future, but it is happening already.

THE BENEFITS AND CAPABILITIES OF FACIAL RECOGNITION

The capability of Facial Recognition Technology (FRT) has progressed significantly over recent years. Previously, FRT required full lighting and high-quality images to recognise an individual on a database. However, the most mature systems on the market now enable the recognition of faces in moving crowds, at extreme angles and with low quality images. Masks also no longer pose an issue to this technology and the best systems can recognise a face in nearly complete darkness. Research and testing by the National Institute of Standards and Technology (NIST) highlights these improvements. For example, as of April 2020, the best face identification algorithm has an error rate of just 0.08% compared to 4.1% for the leading algorithm in 2014.

Further accuracy gains will continue to reduce risks related to misidentification, and expand the benefits that can come from proper use. For instance, this technology will become essential for re-energising the night-time economy. With an integrated Facial Recognition system utilised in venues or night clubs, visitors will be able to gain entry, prove their age and pay for drinks all using their biometric signature rather than ID or credit cards. The benefits to this implementation are three-fold: the customer experience will be streamlined, venue safety improved and business owner revenues increased. To ensure this application is rolled out successfully, all organisations must be transparent with their use of FRT and only use it on an opt-in basis, so that there is no breach of privacy.

Facial Recognition is also one of the key touch-free authentication methods being adopted for access control. Large businesses and workplaces are starting to recognise the value in Facial Recognition to enhance the flow of people through buildings. The most sophisticated systems can authenticate multiple individuals at once rather than needing sight of one individual face at a time, which can reduce overcrowding and streamline entry. Facial Recognition can also protect sensitive locations, admitting only 'whitelist' approved visitors, and thus easing the strain on venue management and security personnel.



THE 'HUMAN IN THE LOOP'

The benefits of Facial Recognition can be far-reaching. However, there are a number of considerations essential to ensuring this technology is only ever used as a force for good.

TONY PORTER
CHIEF PRIVACY OFFICER, CORSIGHT AI

If we look at protecting large entertainment venues as an example, how can this be done safely and ethically?

When classified facilities utilise Live Facial Recognition (LFR) cameras at entry points, the digital signatures of all those entering a venue will be scanned against watchlists. Any biometric data on that watchlist will be that of individuals known by police or security teams as a genuine threat to others. Therefore, once this data is recognised by the LFR cameras, security will be alerted and these teams can decide on their next steps. The key here is to ensure that watchlists are never impermissibly wide – only ever narrowly compiled – and those operating the Facial Recognition systems must be well trained.

In fact, it is highly unethical to develop and implement a FRT system without following a 'human in the loop' strategy, e.g., a trained operator that makes final decisions based on the technology's insight. It is the responsibility of the developer of the Facial Recognition system to make sure that the operator of this technology is appropriately trained and able to comprehend how to interpret results, understand the inherent bias of algorithms and look for the variation in threshold and impact. They also must then recognise how all of these elements may impact the results. This is because, like the majority of technology, FRT is here to support and optimise human capability rather than replace it entirely.

An effective Facial Recognition system will also provide the operator with a myriad of privacy options, and it is their role to deploy them. Operators should be aware that the best solutions on the market allow faces of by-passers to be blurred both in playback and in live video. This means only the biometric data of those on a small watch-list would ever be captured, encouraging a safer, more trusted use of the technology. However, it is the role of the operator to opt-in to this privacy feature and also delete any data if a false positive result occurs. Importantly, it is the responsibility of the developers and resellers of these systems to offer guidance for the operators and data controllers. This can include supporting in the development of a Privacy Management Programme (PMP) as a framework for safe practice, as well as a Data Privacy Impact Assessment Survey (DPIA) consultative service to identify and mitigate any risks to privacy.

LAW AND REGULATION

While there is currently no law that directly regulates Facial Recognition within Australia, there is some legislation around privacy that developers and implementors must follow. The law that best holds FRT to account is Australia's Privacy Act 1988, which provides a set of principles that must be applied when working with personal information.

In future, we're hopeful that further legislation will be introduced so that this technology can finally be used to its safest and best ability. However, it is not just for the technology industry to call for this further regulation. Everyone that is concerned about their privacy should be demanding greater adherence to ethical practices from their technology solutions providers, and they should also be campaigning their government bodies for more regulation to make this possible. Facial Recognition is here to stay, but there needs to be more guidelines to help protect the privacy of the people who are most affected by the technology.

Finally, whilst privacy and ethics must be a top priority, we must still encourage a discussion around Facial Recognition's life-changing benefits. It is time to level the playing field of the FRT debate and talk about the 'force for good' it can offer the security industry as well as wider society.