OPTIC SECURITY GROUP

Executive Brief

Facial Recognition Technology: Understanding Community Expectations

OPTICIQ

Facial Recognition technology (FRT) is developing at a rapid pace, and it offers a range of game-changing security, safety, efficiency, and profitability benefits for organisations. But the technology also presents significant challenges in terms of public acceptability, privacy, and a fast-evolving regulatory landscape.

Several major retailers, for example, have become the subject of media controversies over deployments of FRT that have put them at odds with public expectations around privacy and informed consent. FRT deployments are also frequently falling foul of privacy regulators.

This Executive Brief offers a 'first principles' approach to considering these risks and evaluating the appropriateness of FRT for organisations and the purposes for which they intend to deploy it. Drawing from international empirical research, we provide insights that may assist organisations to mitigate the regulatory and reputational risks associated with FRT missteps.

Context is Key:
Public acceptability of FRT is a technology risk

Why is facial recognition technology (FRT) controversial in some scenarios but widely accepted in others?

Why, for example, have some FRT deployments in retail stores resulted in media controversy, while most of us are happy to have our facial images captured at airport passport control? Why are many of us comfortable using the technology to unlock our smart phones yet uncomfortable about its use in monitoring public spaces?

FRT is a powerful tool that offers many potential security – and other – benefits. But what may be viewed by an organisation as a revolutionary crime prevention and business improvement capability may be viewed by many of its customers or employees as technological overreach and a threat to individual privacy and freedoms.

The recent frequency of FRT missteps and media controversies suggests that organisations looking to install and operate FRT-enabled CCTV need to do more than merely tick the privacy compliance boxes to avoid potential reputational fall-out from an unpopular FRT deployment. They also need to consider the 'public acceptability' of the deployment in order to establish whether they have the social licence to implement it.

In this white paper we explore the international research on FRT public acceptability, which demonstrates that some deployments of FRT are more publicly acceptable than others. This research highlights that there are clear patterns to acceptability depending on the purpose of deployment and – importantly – whether the operator is a government agency, law enforcement, a business, or individual.

An inappropriate FRT deployment exposes the organisation operating it to significant reputational risk - even if the privacy compliance boxes have been ticked. Understanding the deployment-specific patterns of public acceptability of FRT can assist organisations to ensure that they possess the social licence to operate this emerging technology, avoid controversy, and engage with it with confidence.

The Research

In research recently published in the *National Security Journal*, a publication of Massey University's Centre for Defence & Security Studies, I collated 200 data points from 15 international research studies in order to 'map' the public acceptability of a diverse range of FRT deployments.

Drawing from this research, this paper, part of the OpticIQ Executive Brief series, presents key insights into why some deployments of FRT are more acceptable than others, and lists the key factors that organisations should consider when planning their use of the technology.

I hope you derive value from this research, and if you are interested in knowing more about it, do not hesitate to reach out.

Nicholas Dynon
Optic Security Group

OPTICIQ

About the OpticIQ Executive Brief series

Advanced video analytics, facial recognition, artificial intelligence, and surveillance cloud are just some of the emerging technologies shaping tomorrow's security landscape. While they offer potential benefits for the safety and security of organisations, these technologies are both powerful and rapidly evolving, presenting novel challenges and risks.

Optic Security Group assists its customers to navigate this landscape. Via the **OpticIQ Lab** - a sovereign capability for the testing, training, trialling, and commissioning of emerging security technologies - and our tech partnerships, we are developing trusted security solutions for the future.

As an emerging security technology centre of excellence, the OpticIQ Lab periodically publishes Executive Briefs in order to socialise its research and anaylsis and to provide organisational leaders and decision makers with actionable, relevant, evidence-based insights.

1. Individual use of FRT

FRT acceptability data confirms that individuals tend to place trust in the facial recognition technology on their own smart devices. According to a 2019 study, 58.9% of people in the US were comfortable with using facial recognition to unlock their smartphone. A 2024 survey found 68.8% of Australians felt the same.

They're statistics that may seem somewhat counter-intuitive considering that many of these users may report feeling less comfortable about – or even object to – the idea of having their facial image recorded by a public-facing camera.

But, as the data suggests, when an individual uses facial recognition technology on their own phone they *feel* in control – even though they may in fact have little control over how their facial data is being used and who it may end with.

Beyond device unlocking, other individual uses of FRT are associated with lower levels of acceptability. According to a 2016 UK study, 31% of respondents were comfortable with the idea of using FRT to bid in online auctions, and only 24% considered using FRT for contributing to online forums to be acceptable.

Convenience and proportionality are key here. Using one's face to unlock one's device is considered a convenient alternative to unblocking via password or even finger scan. The idea of having to provide one's biometric in order to comment in an online forum, however, is viewed as a disproportionately intrusive measure of little perceived benefit to the user.

Purpose	Where	Acceptance	Year	Country
Verify Identity for applying for ID documents	Device	78.99%	2021	US, UK, AU
Unlock personal technology, e.g., smart phone	Device	68.8%	2024	AU
Age verification for accessing online gambling	Device	60.6%	2024	AU
Identity verification for accessing govt services	Device	57.4%	2024	AU
Logging in to Facebook from a different PC	Device	34%	2016	UK
Topping up public transport card online	Device	31%	2016	UK
Contributing to an online forum	Device	24%	2016	UK

Table 1: Selected research data on public acceptance of individual FRT operation.

2. Government use of FRT

Just like individual use of facial recognition technology, public acceptance of government use of RFT varies greatly depending on the purpose for which it is being used. There are a few reasons for this:

Familiarity: The rule of thumb that the more familiar people are with a particular technology the higher their level of acceptance of it tends to be tends to hold true in relation to FRT. The research data tells us, for example, that people tend to be relatively comfortable with the now commonplace use of facial recognition for identifying passengers at airport customs. When it comes to less familiar deployments, such as identifying voters at polling places, it's a different story.

Proportionality: People generally accept the use of facial recognition technology by police to identify terrorists and investigate serious crimes but are resistant to it being used to identify minor offences and antisocial behaviours, such as parking violations and littering.

Specificity: The more ambiguous the use of the technology is, the greater the degree of discomfort around it. Deployments such as "monitoring crowds as they walk down the street" and "day-to-day policing" lead to concerns over ubiquitous surveillance and the loss of "practical obscurity".

Purpose	Where	Acceptance	Year	Country
Search for persons who've committed crime	Open	88.86%	2021	US, UK, AU
Search for missing persons	Open	86.08%	2021	US, UK, AU
Border security	Airports	76%	2020	AU
Traffic violations and enforcement	Open	51%	2020	AU
Access to school building and grounds	Schools	48%	2020	AU
Identify people for minor offences	Open	47%	2020	AU
Track student attendance	Schools	43%	2022	US

Table 2: Selected research data on public acceptance of government/law enforcement FRT operation.

3. Private sector use of FRT

A key finding of the research data is that people are generally less accepting of FRT cameras when they are operated by private sector organisations. In short, people place little trust in businesses' ability to operate the technology responsibly or to the benefit of the public.

The use of FRT by retailers to identify known shoplifters and antisocial patrons, for example, is considered no more acceptable by the public than the idea of police using FRT to identify minor offenders or traffic rule breakers.

That being said, the public is more accepting of retailers' use of FRT to identify shoplifters, antisocial patrons and fraudsters than it is of its use by retailers for other purposes – such as loyalty programs, advertising, payments and the tracking of customer behaviour.

The public acceptability of FRT operation by businesses in other contexts echoes the patterns we see in the retail setting. In gaming venues, for example, the use of facial recognition for age verification or to identify self-excluded gamblers is more accepted than its use in identifying VIP gamblers for customer experience or marketing purposes.

In the workplace, the identification of thieves through FRT attracts limited although greater acceptance than uses relating to employee location and behaviour tracking.

Purpose	Where	Acceptance	Year	Country
Detect known shoplifters	Retail	58.9%	2023	US
Identify individuals banned from store	Retail	54.8%	2022	US
Identify shoplifters and antisocial patrons	Retail	54.4%	2024	AU
Blacklist people who've behaved antisocially	Retail	36.71%	2021	US, UK, AU
Collect demographic information on shoppers	Retail	19.4%	2024	AU
Customise advertising to individual shoppers	Retail	15.7%	2024	AU
Shopper behaviour tracking in supermarkets	Retail	7%	2019	UK

Table 3: Selected research data on public acceptance of FRT operation by retailers.

4. Risk and Reward

Ultimately, the research data tells us that public acceptability of FRT tends to involve a range of trade-offs between *risks* and *rewards*.

Individuals may be willing to accept the risks involved with providing their facial data to an FRT operator where they perceive a potential (i) direct benefit, such as greater convenience, faster service, or privileged access to a restricted area, or (ii) indirect (public) benefit, such as safer international borders, safeguarding of national security, or a decrease in serious crime.

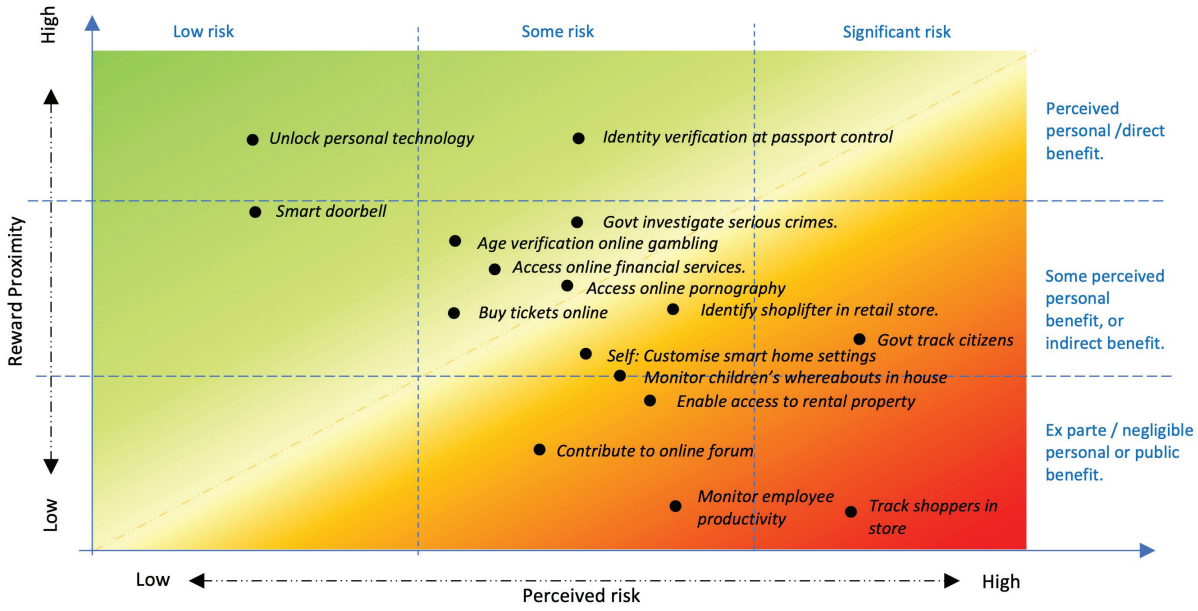
Whereas the use of FRT by police to investigate crime may be seen as 'rewarding' in terms of delivering a public benefit, the use of FRT by private businesses – even when it is purportedly for the purpose of crime prevention – tends to be seen as self-serving and holding little or no reward to those being surveilled.

In addition to the rewards, the risk calculus is heavily influenced by who the operator is, and what they are using the technology for.

Private businesses are generally perceived as 'riskier' FRT operators compared to government; and less familiar, less specific, and less proportionate uses of the technology are perceived as relatively risky.

A risk/reward approach provides us with a framework for plotting the indicative relative acceptability of various FRT deployments - as demonstrated in the *FRT Public Acceptability Model* below.

The FRT Public Acceptability Model



The above model provides a simple framework for understanding the indicative public acceptability of various FRT deployments based on what the existing research tells us.

In this model, 'risk' forms the x-axis while 'reward' constitutes the y-axis. Graduations along each axis intersect, forming a matrix made up of segments that each correspond to distinct risk/reward combinations - from low risk/high reward in the top left to high risk/low reward in the bottom right.

From the bottom left to the top right is a trade-off line along which risk and reward are at – or close to – equilibrium.

Various examples of FRT deployments may be plotted in the matrix based on an approximation of the levels of risk and reward attributed to them in the research..

The further a plotted deployment is above the trade-off line, the more confidence one may have that it falls within the realm of publicly acceptability, while the further a deployment is below the trade-off line, the higher the confidence one may have that it would meet with unacceptability.

5. Key Takeaways:
A first principles approach

FRT continues to develop – and improve – rapidly. But it is a technology that's 100% dependent on its ability to extract unique biometric information from individuals' bodies – and their being okay with that. This makes it a particularly sensitive technology that should be approached with care.

Organisations looking to operate FRT to enhance their security should seek to confirm whether they have a Social Licence to Operate (SLO) the technology for the purpose(s) and way(s) they intend to deploy it.

SLO refers to the level of acceptance or approval by local communities and stakeholders of organisations and their operations, and is based on the idea that organisations need not only regulatory permission but also 'social permission' to conduct their operations.

Establishing Social Licence to Operate should form part of a 'first principles' approach to informing whether an FRT deployment – despite its potential benefits – presents unacceptable risks to the organisation. The following four questions provide a good place to start:

1. Is FRT the best solution for your needs?

Organisations often narrowly focus on what security hardware and software they have deployed as a measure of how protected they are, and new technologies can often be seen as a silver bullet. But is FRT the best solution to achieve your security objectives?

In other words, can the same outcome be achieved with a different type of solution?

While FRT, for example, may provide an automated solution for age verification at gaming and licenced premises, it may not necessarily deliver all the security and safety benefits that a verbal exchange between staff and patron may provide.

Where FRT is being considered for the purposes of tracking visitors through restricted areas of a building, are there other smart solutions available that don't necessitate the recording and storage of facial biometric data?

2. What supporting security controls will you need?

Even the best security controls rarely work well in isolation. Good security is achieved when multiple security controls work together to protect an asset. If you have assessed that FRT is the most effective solution to your security problem, then consider what other controls you will also need to support it.

Live facial recognition, for example, is a powerful security control, but it's not effective on its own. It achieves optimal security outcomes when integrated with a range of supporting controls, such as strong security policies and processes, trained and aware staff, physical barriers and (potentially) access control, responsive security personnel, and/or a timely law enforcement response. Without these, the tech may at best end up a white elephant or at worst create conflict situations that may place staff in harm's way.

5. Key Takeaways [continued]

3. What are your privacy and ethical obligations?

Understand your privacy and data protection obligations. Facial biometric data is a personal identifier that is unique to an individual, and it must be handled in accordance with privacy and data protection legislation. A thorough understanding of the legislation includes other relevant material, such as guidance documents and determinations handed down by the Australian Privacy Commissioner.

In addition to the legislation, get to know (and stay up to date with) relevant standards and codes of practice for CCTV, biometrics, facial recognition, and artificial intelligence where they exist. These may include resources published by:

- International bodies, such as the Internationa Organisation for Standardisation (*ISO/IEC 42001:2023 - AI management systems*), Responsible Artificial Intelligence Institute, and OECD Global Partnership on Artificial Intelligence, among others;
- Australian Government, including the *Policy for responsible use of AI in government*, *National framework for the assurance of artificial intelligence in government*, *Voluntary AI Safety Standard*; and
- Industry bodies, such as ASIAL (*Guidling principles for Artificial Intelligence and the ethical use of Automated Facial Recognition*), Biometrics Institute (*Ethical Principles for Biometrics*), etc.

4. How publicly acceptable is your FRT deployment?

Take an Enterprise Risk Management approach to considering the feasibility of FRT for your organisation.

While FRT may pose an attractive solution to managing your security risks, will it unintentionally expose your organisation to reputational risk? An understanding of the public acceptability of your intended FRT deployment is a critical step in assessing the potential reputational risk of the deployment.

Deploying FRT in a retail context for the sole (or secondary) purpose of advertising and loyalty program-related shopper tracking may result in customer backlash and a potential public relations nightmare. Deploying FRT in contexts involving vulnerable groups, such as children and the elderly, require particularly careful consideration.

While resources such as the *FRT Public Acceptability Model* and the research that informs it provide a good evidence basis to start from, you should consider whether other methods of researching the acceptability of your intended FRT deployment are warranted. These may include surveys, interviews, or other mechanisms for consulting with stakeholders - or engaging an independent party to do so on your behalf.

About the Author

Nicholas Dynon is Group Brand Strategy & Innovation Director at Optic Security Group. Nick previously served with the Australian Government Department of Home Affairs, including in diplomatic missions in China and the Pacific, and has since worked for over a decade in enterprise security. He is a founding member of the Massey University *National Security Journal* editorial board, Chief Editor of the *New Zealand Security Magazine*, and a respected security researcher and commentator.

A graduate of the Royal Military College of Australia, Nick holds a B.A. Hons and M.A. (ANU), and a Master of International Studies Hons (Sydney). He is a licensed Security Consultant, Certified Counter Terrorism Practitioner, and recipient of the 2022 New Zealand Outstanding Security Performance Award (OSPA) for Lifetime Achievement.

nicholas.dynon@opticsecuritygroup.com

About Optic Security Group

Optic Security Group provides converged security risk management solutions serving the needs of enterprise and government clients across Australia and New Zealand. Optic specialises in services and solutions that enable its clients to achieve resilience to multi-domain digital-physical security risks.

Optic delivers end-to-end security risk management through security risk advisory; networked and integrated physical security and safety system design, installation, monitoring, servicing, and maintenance; information and cybersecurity solutions.

OpticIQ, a division of Optic Security Group, is focused on the research and development of emerging security technologies, and on advisory in relation to techology risk and Responsible AI. The Adelaide-based OpticIQ Lab provides a sovereign capability for the development, testing, training, and deployment readying of emerging analytic and AI-enabled technologies.

Key Sources:

Dynon, N. (2024). Licence to Operate: Mapping the Public Acceptability of Facial Recognition Technology. National Security Journal. Published 20 October 2024.
Dynon, N. (2024). In your face: our acceptance of facial recognition technology depends on who is doing it – and where. The Conversation, Published 08 November 2024.

Please Note:

The information contained in this white paper does not constitute professional advice. The information is of a general nature only and readers seeking advice of a specialised nature should consult with a professional. The data referred to in this Brief should be considered as indicative only as it draws from several distinct studies conducted at different times and among different respondent populations.

OPTIC SECURITY GROUP

OPTICIQ

www.opticsecuritygroup.com
australia@opticsecuritygroup.com
nz@opticsecuritygroup.com

Last updated 06 February 2025
Images courtesy of Unsplash.