National Security Journal

http://nationalsecurityjournal.nz

Published by:
Centre for Defence
and Security Studies,
Massey University

ISSN: 2703-1926 (print)   ISSN: 2703-1934 (online)

Licence to Operate: Mapping the Public Acceptability of Facial Recognition Technology

Author: Dynon, Nicholas

To cite this article: Dynon, N. (2024). Licence to Operate: Mapping the Public Acceptability of Facial Recognition Technology. *National Security Journal*. Published 20 October 2024. doi: 10.36878/nsj20241020.06

To link to this article: https://doi.org/10.36878/nsj20241020.06

View CrossRef data: http://search.crossref.org/?q=10.36878%2Fnsj20241020.06

Journal Article published 20 October 2024 in National Security Journal.

LICENCE TO OPERATE: MAPPING THE PUBLIC ACCEPTABILITY OF FACIAL RECOGNITION TECHNOLOGY

Nicholas Dynon[1]

Rapid developments in facial recognition technology (FRT) have made its use in contemporary surveillance-oriented security technology (SOST) systems, such as CCTV, increasingly widespread. An artificial intelligence-based technology, FRT is a force multiplier for these systems, delivering security, efficiency and business intelligence gains for organisations that deploy it. At the same time, it is a controversial technology, but unevenly so. Publics tend to accept that the technology has become part of the process of passing through customs at airports, for example, yet its use by retailers has sparked frequent backlash. The frequency of these controversies suggests that security consultants and other practitioners responsible for providing advice to organisations in relation to the suitability of security systems are failing to incorporate the 'public acceptability' of potential FRT deployments within their advice. Existing research on FRT public acceptability demonstrates that some deployments of FRT are more publicly acceptable than others. This paper collates the data from existing FRT public acceptability research in order to (i) identify deployment-specific patterns of acceptability, and (ii) develop a model for mapping the acceptability of potential deployments based on a 'reward proximity' versus 'perceived risk' trade-off. This model may assist actors within the FRT supply chain to make more informed choices in relation to the appropriateness of facial recognition technology in specific deployment scenarios.

Keywords: Facial Recognition Technology, biometrics, live facial recognition, surveillance-oriented security technologies, video surveillance, analytics, CCTV, emerging technology.

[1] The author is Innovation & Risk Manager at Optic Security Group. Address for correspondence: nicholas.dynon@opticsecuritygroup.com. He wishes to acknowledge two anonymous reviewers, NSJ Managing Editor Dr John Battersby, and Andrew Thorburn, for their comments on drafts.

Introduction

Deployments of live Facial Recognition Technology[2] (FRT) by retailers in New Zealand and Australia have in recent years elicited national media attention – often for the wrong reasons. In a few short years, rapid developments in CCTV[3] video analytics have led to a proliferation of FRT deployments amid concerns over its intrusiveness, its accuracy, apparent biases in relation to women and minorities, the lack of transparency around its growth, and the absence of safeguards and legislation regulating its use. Internationally, communities are largely unclear as to exactly what FRT is capable of, and are broadly split down the middle in their acceptance of it. What makes the technology all the more controversial is that in spite of this, we're nevertheless witnessing a proliferation in its deployment in more of the spaces we frequent in the course of our daily lives.

Debates in New Zealand and Australia around FRT – and particularly live FRT – are recent relative to comparable jurisdictions internationally. Public discourse on FRT in the UK and US, for example, has been longer running, wider ranging, and higher in profile. In these jurisdictions, significant FRT deployments by law enforcement, government agencies, and the private sector have occurred in the absence of legislation specifically allowing, prohibiting, or identifying limits to them. In this void, limited numbers of sub-state actors, including some municipal authorities and universities, have stepped in to limit or ban the deployment of FRT within their jurisdictions, and many lobby groups have acted to mobilise opposition to what they perceive as a disproportionately intrusive surveillance-oriented security technology (SOST).[4] The technological innovations that underpin FRT have been developed in the absence of public awareness, political debate, and legislative accommodation, and – echoing international experience – this has led to recent controversies in both New Zealand and Australia.

New Zealand supermarket cooperative Foodstuffs North Island Limited commenced a six-month trial of FRT across 25 of its New World and Pak'n Save supermarkets in February 2024. Citing historically high rates of retail crime across its stores, Foodstuffs looked to the tech's ability to identify Persons of Interest from among shoppers entering its stores.[1] This followed a reported 29-store trial in late 2022 in which the company refused to confirm which of its stores were involved,[2] in addition to earlier discrete deployments that had made it to the media as far back as 2018.[3] Only several weeks into

[2] Facial Recognition Technology includes a wide range of machine-vision-based technologies capable of enrolling, collecting, matching, and analysing the facial features of an individual as a unique biometric identifier. Matching may either involve a one-to-one match of an individual's facial biometric to a copy of their biometric stored in a database, or a one-to-many match of an individual's biometric against any number of stored biometric records. The matching process may occur 'live' (as facial images are captured by a camera in real time) or 'historically' (from previously recorded camera footage).

[3] CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are recorded, and often monitored, usually for surveillance and security purposes.

[4] In the US, for example, the Fight For the Future group, has released a list of music festivals that have pledged to never employ biometric technologies for ticketing or security purposes at their event. https://festivals.banfacialrecognition.com/

the 2024 trial, news reports emerged of a Māori mother feeling “racially discriminated” against after being misidentified as a trespassed thief at a participating Rotorua New World supermarket.[4] In the wake of the incident, University of Canterbury lecturer Mark Rickerby commented that the company’s response that it was a “genuine case of human error”, failed to address “deeper questions about such use of AI and automated systems.”[5] Given the procedures listed for the trial (two authorised store personnel must verify the accuracy of the FRT system match), it is likely that the ‘human error’ occurred only after the facial recognition software had already flagged the individual as a match (a false positive)[5] – and that therefore the error originated with the (90% accurate) algorithm.[6] It’s not the first time the company had invoked the ‘human error’ line in its communications, suggesting a reluctance to blame the technology. In an unprecedented move, the Privacy Commissioner initiated an inquiry into the trial.[7] The other member of New Zealand’s supermarket duopoly, Woolworths New Zealand (formerly Progressive Enterprises Limited), has looked past FRT to alternative technologies to stem crime and antisocial behaviours in its stores, deploying body-worn cameras (BWCs) to its staff in April 2024.[8] Concerns that its BWCs may include FRT prompted the company to issue a media release confirming that it does not use facial recognition technology in any of its stores.[9]

In Australia, a finding by consumer watchdog CHOICE that Bunnings, Kmart, and The Good Guys may have breached the Privacy Act with their use of FRT resulted in the retailers pausing their use of the technology in July 2022 after a public backlash. It also prompted the Office of the Australian Information Commissioner (OAIC) to open an investigation into their use of the technology.[10] The probe into The Good Guys was dropped when the company “suspended their use of facial recognition technology and indicated that they weren’t intending to reinstate it”.[11] Earlier, in an October 2021 FRT-related investigation, Australian Information Commissioner and Privacy Commissioner Angelene Falk found that convenience store group 7-Eleven had “interfered with customers’ privacy by collecting sensitive biometric information that was not reasonably necessary for its functions and without adequate notice or consent”.[12]

In both New Zealand and Australia police deployment of FRT hit the headlines in 2020 when their respective uses of Clearview AI were revealed. There was uproar when it was found that New Zealand Police had conducted a trial of the controversial software without consulting either its own leadership or the Privacy Commissioner.[13] In December 2021, responding to an independent expert review into the matter, Police publicly stated that “it will not use live Facial Recognition technology without further detailed analysis, taking account of legal, privacy and human rights concerns – with a particular focus on the New Zealand context.”[14] More recently, New Zealand Police published their

[5] False positives are instances where the FRT algorithm matches a query image with a face from the known-faces database erroneously, potentially matching a person’s face with that of a person of interest (e.g. a black-listed person or criminal), which could result in negative outcomes for members of the public.

first-ever policy on facial recognition, placing a stop on police deployment of Live FRT in all but rare and extreme circumstances, stating that "in the New Zealand context, it is considered that the overall risks of live FRT outweigh the potential benefits". The policy, released in August, places safeguards on a range of other authorised police uses of FRT.[15] Controversy similarly plagued the Australian Federal Police's (AFP) deployment of the technology in 2020 with its use of Clearview AI and Auror analytics.[16] The AFP suspended its use of Auror (a retail crime intelligence platform with FRT functionality) in 2023 only after a freedom of information (FOI) request revealed that more than 100 of its staff had used the platform without considering privacy or security implications.[17]

In apparent contradiction, many other FRT deployments raise remarkably fewer concerns. "Facial recognition is widely accepted in some forms," note Doberstein, *et al.*, "like in playful social media apps or when sorting photos into automated digital albums, and resisted in other forms, such as when police forces use it."[18] The public is more familiar and 'okay' with certain FRT deployments, such as when unlocking one's own smart phone or passing through eGates / SmartGates at airport passport control, while other deployments – although less familiar – just seem to make inherent sense, such as in the post-incident investigation of a mass shooting or in the verification of an individual's identity who has lost their documents in conflict or natural disaster. In short, some FRT deployments appear to be either more or less controversial than others, and where a specific deployment creates significant controversy it suggests a failure of the FRT operator and their supply chain to have adequately assessed the potential (i) level of public acceptability of their intended deployment, or (ii) reputational risks stemming from a deployment type known to attract low levels of public acceptability (or high levels of non-acceptance).

This has important implications for all parties within the FRT supply chain, from CCTV manufacturers and video analytics developers to security system hardware and software distributors, security consultants, security integrators/installers, and to the organisations that purchase and operate the technology. Fearing public backlash, purchasing organisations may be scared away from considering FRT deployments altogether, or, not anticipating controversy, they may invest in wide-scale FRT systems only to inadvertently trigger a major backlash and expose themselves to a range of unintended consequences.[19] Yet the number of deployments that have resulted in media controversy suggest that in the absence of regulation, FRT vendors remain overwhelmingly driven by sales imperatives while security consultants and purchasers remain underwhelmingly knowledgeable in relation to FRT public acceptability factors.

The deployment of live FRT by casinos to identify and prohibit entry to self-declared problem gamblers is a case in point.[20] One the one hand, this deployment type receives strong support by many governments and broad public acceptance, yet, on the other hand, surveillance technology suppliers tend to promote to casinos the ability of FRT tracking to support marketing and player incentive schemes, which are uses that the majority of the public find unacceptable – and which might fall into the trope of 'surveillance capitalism' articulated by Shoshana Zuboff in her seminal work.[21] As recently as 27 March 2024, for example, an Australian Capital Territory Legislative Assembly inquiry into cashless gambling noted that there is an "abundance of industry trade papers and promotional materials for facial recognition technology that makes clear the marketing and profit maximisation benefits such technology offers for casino and other gambling venues".[22] Such dual-use messaging by vendors creates dissonance, and raises the spectre of 'function creep'. While casino operators may see the added value of FRT for marketing and customer loyalty purposes, the majority of their customers are likely be opposed to their facial image being collected for such purposes. Additionally, a casino using its FRT for player incentivisation – in addition to problem gambler prohibition – may unwittingly take on reputational risk if it does so ignorant of the extent of likely negative public sentiment towards it. A resulting controversy may lead not only to brand damage but also to an impact on revenues and losses associated with investment into a FRT system that it may be required to ultimately shut down.

There appears to be a significant mismatch between the proliferating functionalities and use cases of FRT technology promoted by suppliers and the varying levels of public awareness and acceptability of these – and the ability of the FRT supply chain to mediate between the two. What may be extolled by an FRT marketer as a revolutionary crime prevention capability that can also collect data for business improvement and profitability may be viewed by significant segments of the population as technological overreach and a dystopic threat to individual privacy and freedoms. Additionally, the apparent success of FRT in one type of deployment may be used as part of a justification for a system's use in an altogether disparate type of deployment. In the case of the aforementioned Foodstuffs North Island Limited FRT trial, for example, the FRT system used is touted as having been evaluated and endorsed by the South Australian Attorney-General's Department "as an approved FRT system to identify previous barred patrons in gaming venues to prevent the recurrence of problem gambling".[23] From an *operator* perspective the use of FRT in identifying Persons of Interest in supermarkets may appear consistent with its use in identifying barred patrons in gaming venues, but research data indicates that from a *public acceptability* perspective these two scenarios are inconsistent (refer *Table 12* and *Table 14*).

New technology and social acceptance

Survey-based studies conducted in both New Zealand and Australia during 2024 appear to validate the media reportage pointing to societal ambivalence over FRT. A biennial privacy survey of 1,200 New Zealanders released in May by the Office of the Privacy Commissioner found that 49% of respondents were concerned or very concerned about the use of FRT in retail stores to identify individuals. A total of 22% were neutral on the topic, 25% were either not concerned or not really concerned, and 11% were unsure.[24] A total of 64% also said they were very concerned about not being told about or agreeing to the use of FRT. Māori were more likely to express concern about bias in facial recognition (63%) and its use in retail stores (55%). "Increasing public awareness about the use of Facial Recognition Technology and some of the issues being expressed about it seem to be a having an impact," stated Privacy Commissioner Michael Webster, "as people become aware that this is happening and start asking, "is this the society I really want to live in?"[25] In Australia, a Monash University survey conducted in April and May 2024 found the Australian public divided over the likely impact of FRT. A total of 29.5% of respondents agreed that society would be 'better off' or 'much better off' if there is widespread use of facial recognition technology in ten years' time, while 28.6% expressed the opposite opinion.[26] A total of 26.7% of respondents said that it is too early to predict the impact that FRT might have on society and social relations. Both surveys exhibit consistencies with international academic research on FRT public acceptability (see next section), which indicates that acceptability is contingent upon whether the technology is being operated by individuals, government, or private sector organisations, and for what purpose.

Various models have been adopted by researchers in their attempts to understand and measure the extent of social acceptance, or public acceptability, of FRT. These include various iterations of the Technology Acceptance Model (TAM) as well as other frameworks often based on a security-liberty trade-off. Complicating – and perhaps undermining – these efforts is the reality that although there are high levels of awareness of FRT among publics, there are generally very low levels of public understanding of (or familiarity with) it. A 2019 Ada Lovelace Institute study into public attitudes to FRT in the UK found that 46% of people didn't know anything about FRT and a further 48% only knew a little about it.[27] A 2019 Pew Research Center study found that 25% of people in the US knew a lot about FRT, 61% knew a little, and 13% knew nothing.[28] In Australia the abovementioned Monash University study revealed that almost three quarters of Australians say they know little about facial recognition technology. Although 98.9% of respondents were aware of the term, only one in 20 felt they knew "a lot" about it.[29] These results are also supported by a 2021 multi-country study that found that less than 10% of people in the UK and Australia knew a lot about FRT (around 20% in the US), and that over 30% didn't know anything about it.[30] Interestingly, another multi-country study found not only that 92% of respondents had "heard about FRT", but that only 12% of respondents had not personally observed FRT being used in a private or public context.[31]

Developed by Fred Davis as an extension of Ajzen and Fishbein's theory of reasoned action, TAM is widely used to explain users' acceptance of new technologies and products. The model combines 'external variables' (such as age, gender, and social norms) with 'perceived usefulness' (the extent to which users believe that using a specific system will improve their job performance) and 'perceived ease of use' (the ease with which users think a particular system can be used) to identify one's attitude towards and 'behavioral intention to use' a technology.[32] Kostka, *et al*. developed a variant of TAM to demonstrate varying levels of acceptance of FRT in the US (48%), UK (50%), Germany (38%), and China (67%), based on user socio-demographic factors, user experience of the technology, and perceived risks, benefits, usefulness, and reliability.[33] Interestingly, they also found in-country regional variations in acceptance. In a study on FRT and privacy in China, Liu, *et al*. employ a variant of TAM to conclude that perceived usefulness of FRT tends to prevail where risk perceptions around privacy are mitigated by the instillation of a sense of trust in the technology and provider.[34] Nakisa, *et al*. examine the applicability of the TAM in analysing users' perception and attitudes towards the adoption of the facial authentication technology in self-service applications,[35] finding that in order to maintain user trust in relation to FRT it is necessary to develop policies and regulations to protect users "before launching the product into the market".[36] Despite its wide use in relation to FRT acceptance, however, TAM has been criticised for being inherently limited and impractical, and its relevance for SOSTs – as opposed to user-focused information systems – has been questioned. TAM-based models were, after all, developed originally to assess acceptance of information technologies by active users in the workplace, rather than by the passive subjects of FRT surveillance.[37]

According to Pavone, *et al*., public perception studies focused on SOSTs tend to be traditionally framed in terms of a mutually exclusive relationship between security and privacy (or individual rights or liberty) or, in other words, an assumed security-privacy trade-off.[38] These studies are invariably informed by the authoritative and widely recognised works of Michel Foucault on the biophysics of power (biopower), carceral culture, and panoptic surveillance, which link ubiquitous surveillance not only with loss of privacy but also the subjugation of free will (the 'chilling effect').[39] But the trade-off-based studies are also the subject of criticisms. Pavone, *et al*., for example, point out that there is an absence of empirical evidence to support the trade-off assumption. "Public assessment of privacy and security issues associated with the introduction of new SOSTs is not only more complex than the trade-off assumes," they write, "it is also largely affected by a variety of factors, which relate to how these technologies address social priorities and to the social and institutional context of implementation", such as citizens' confidence in the institutions using the technology.[40] The emphasis on the trade-off approach, they argue, "purposively obscures" a range of ethical, social, and political implications associated with the introduction of new SOSTs. Laufs and Borrion argue that while philosophical debates over the tensions between security and individual rights are crucial, they nevertheless deepen the divide between practitioners aiming to improve security and citizens concerned about their privacy rights, and in doing so they neglect on-the-ground outcomes and the role of digital transformation in improving effectiveness and accountability. [41]

Laufs and Borrion also point out that public support for crime reduction measures "fluctuates over time and often as a result of critical events".[42] Support may increase in the direct aftermath of mass-casualty events, for example, and decrease in the wake of a privacy breach or surveillance scandal. According to Andrejevic, *et al*., the COVID-19 pandemic provided opportunities for FRT and other forms of biometric monitoring to expand into new markets.[43] They observed the way in which the security industry, as seen in the conduct of industry trade shows, pivoted to offering biometric solutions to the varied problems of managing state-imposed COVID lock-down, social distancing, and personal hygiene requirements. Such perspectives align with threads of critical security theory, and in particular to the theory of securitisation developed by Ole Waever, Barry Buzan, Jaap de Wilde, and others.[44] Securitisation occurs when an actor attempts to characterise a topic as a security problem where it hadn't previously been regarded as such, and in doing so constructs a context that legitimates the use of extraordinary means to address it. Often-cited examples of this include post-9/11 securitisation, which provided a context for enhanced border surveillance measures (securitisation of borders), and COVID-19, which saw the ushering in of tracer apps that hitherto may have been considered disproportionately intrusive (securitisation of circulation).[45] While critical security theorists may see these examples as demonstrating the role of securitisation in providing a discursive pretext for increased public acceptability of SOSTs, Wester and Giescke argue that this doesn't necessarily bear out. According to their research, in the aftermath of a terrorist attack (or other societal security threat), public opinion doesn't actually sway a great deal.[46] "Instead, citizens differentiate between technologies and owners of systems. "Surveillance technologies", they conclude, "are seen as positive in certain contexts, and not in others".[47]

The COVID-19 pandemic has also been discussed in terms of an often-invoked trade-off between privacy and *convenience*. As Andrejevic, *et al*. note, a "society where one is always recognised might be seen as a convenience for some, but as a threat to others".[48] This trade-off is also reflected in TAM-based FRT acceptability research where convenience is considered as one of many 'perceived effectiveness' factors. Guleria, *et al*. note that with a drive towards contactless tech in the wake of the COVID-19 pandemic, FRT's popularity has risen due to its contactless biometric characteristics. "Businesses are replacing conventional fingerprint scanners with artificial intelligence based FRT," they observe, "opening up enormous commercial prospects." They cite security and surveillance, authentication, access control, and digital healthcare as sectors where its use has become essential.[49] But, like security versus privacy, the convenience versus privacy trade-off approach has its limitations. While convenience may be a relevant acceptance factor for an individual operating FRT to unlock their mobile device, that same individual is most unlikely to cite convenience as a factor in their attitudes towards being filmed by live FRT surveillance in a public place.

FRT acceptability is deployment-specific

A wide range of variables that affect public acceptability of FRT can be discerned from the existing research literature, from (i) *personal factors* (nationality, age, gender, demographics, familiarity with and prior exposure to FRT, ideological outlook, level of trust in others, and perceptions of the technology in relation to privacy, accuracy, and racial bias), to (ii) *social factors* (trust in government and institutions, culturally-specific conceptions of privacy), to (iii) *technological factors* (country of origin, performance, reliability and accuracy, and security of data), and (iv) *deployment factors* (operator, purpose, one-to-one versus one-to-many, live vs historical, type of location, opt-outs, and safeguards). Of these, deployment factors have received the least attention. Yet, as Esposti and Gómez assert in relation to CCTV, citizens' perceptions of the institutional context in which the technology is installed "makes a fundamental difference in the kind of considerations made".[50] Similiarly, as Andrejevic *et al*. point out, "the public can possess different attitudes to FRT in terms of its acceptability (or otherwise) depending on the specifics of the use case", a point also emphasised by both Kugler and Ritchie.[51] Finally, as Wester and Giescke suggest, SOSTs are seen as positive in certain contexts, and not in others. In short, context matters.

As the following discussion will evidence, existing research supports the proposition that acceptability of FRT is ultimately deployment specific. In other words, why some FRT deployments are controversial and some are not is contingent upon *who* is operating the FRT, *why* it is being operated, *where* it is being operated, and *how*:

- *Who:* individuals (smartphones and personal computing devices), government (including law enforcement), or private companies.
- *Why:* identity verification, service enrolment, access to premises, denial of access to premises, live matching with person of interest database, criminal investigation.
- *Where:* own device, restricted area (airport passport control, casino, defence facility), venue, public space, workplace, privately owned public space, shopping malls and retail stores.
- *How:* one-to-one versus one-to-many, live matching versus historical matching, local versus national database.

Understanding the public acceptability of FRT in this way is a useful departure from much of the existing scholarship not least because deployment factors are 'on-the-ground' considerations that are readily understood by relevant actors in the FRT supply chain. In the case of the video surveillance (CCTV) market, these actors include FRT device manufacturers, security system distributors, security consultants (advisers), security system integrators (installers), and security managers within organisations that purchase and operate FRT. Apart from the latter group, the most relevant of these are arguably the licensed security consultants that liaise directly with device buyers/operators. In the statutory licensing regimes of New Zealand and Australia's states and territories, private 'security consultants' or 'security advisers' are invariably defined as persons who, among other things, perform an advisory role in relation to the 'desirability' of security equipment or who 'provide advice' in relation to security equipment and other security controls.[6] Where they are members of recognised industry (NZSA in New Zealand and ASIAL in Australia) or professional associations (such as ASIS International, International Association of Professional Security Consultants, International Code of Conduct Association) – or holders of certifications issued by such organisations – they may be subject to additional independence and/or ethical and professional requirements that set expectations of them in terms of providing objective counsel to their clients in relation to the appropriateness of a security solution. It is these actors who are the most aptly placed of all parties within the SOST supply chain to advise buyers in relation to the appropriateness of an FRT deployment and whether a deployment may struggle to achieve public acceptability. Ideally, purchasers/operators should maintain knowledge of currents in FRT acceptability and ensure that this informs risk-based decisions around SOST selection.

The following discussion considers a broad selection of available recent empirical research conducted into the public acceptability of specific FRT deployment scenarios. Only survey-based studies that present acceptability as a percentage of total responses in relation to specific deployment scenarios are used, as opposed to studies that either do not present acceptability as a percentage or do so without being deployment-specific. It is important to note that each of these studies follow distinct methodologies, including using distinct definitions of or proxies for acceptability (acceptance, comfort, agreement), different survey populations (US, UK, Australia, etc.), and presenting deployment types in different ways (either using real world examples, vignettes, or abstractions). As such, caution is recommended in making anything more than indicative comparisons between the displayed percentages where they come from different studies.

The discussion is structured according to a typology of FRT operators that includes (i) individuals, (ii) government agencies, and (iii) private companies. This typology has been chosen because the reviewed research attaches distinct acceptability profiles to each of these. Eposti and Gómez, for example, note that it is important to distinguish whether cameras are managed by public authorities or by private entities and for what purpose, with video surveillance carried out by public authorities widely more accepted than that carried out by private companies.[52] Echoing this, Ritchie, *et al*. find that publics in the UK, Australia and China trust police (58.37%) and government (42.93%)

[6] For New Zealand, refer to the *Private Security Personnel & Private Investigators Act 2010*, Part 1, Section 7 – Meaning of Security Consultant. For Australia, refer to state and territory-specific private security licensing legislation.

more than private companies (17.50%) to operate FRT.[53] According to Kostka *et al*., acceptance is highest for individuals' own use of FRT (China 71%, US 52%, UK 50%, Germany 33%), then government (China 51%, US 37%, UK 42%, Germany 38%), then private companies (China 17%, US 30%, UK 20%, Germany 15%).[54] Broadly speaking, the public acceptability of individuals' operation of FRT on their own device is associated with low levels of perceived risk (they trust themselves) and often high levels of perceived reward (they derive direct benefit from it, such as convenience). Government agencies' operation of FRT is associated with mixed levels of perceived risk (it depends on what it's being used for, and how) and perceived reward (there is perceived direct (personal) benefit in certain use cases, such as passing quickly through airport border checks, and perceived indirect (public) benefit in others, such as fighting crime and thwarting terrorists. Lastly, private companies' operation of FRT tends to be associated with relatively higher levels of risk, and often lower levels of perceived reward for surveilled individuals.

(i) Individual as Operator

Perhaps among the most curious findings within the research are the relatively high levels of trust individuals have in the FRT they interact with on their own smart phones and devices. This is curious because although individuals physically 'operate' the technology by engaging with it via an app on their phone, the app itself is made available and operated by either a private company (device manufacturer, third party authenticator, or service provider) or a government agency. It's a curiosity that many security practitioners find perverse, often prompting them to question how individuals can be relatively untrusting of FRT's use in CCTV cameras despite using it on their phone cameras all the time. While it may seem contradictory, it highlights that acceptance is a product of perception, and when an individual uses FRT on their own phone they *feel* in control. So disparate is the widespread acceptance of individual FRT operation to that of government and private sector operation that the Electronic Frontier Foundation, a leading US-based digital civil liberties nonprofit organisation, publicly states that it does not support banning private use of the technology despite pushing for curbs on government and private sector use.[55]

Widely accepted personal uses of FRT include unlocking one's smartphone or using an app in a device to verify one's identity in order to access a service (such as one's bank account or government online services). A total of 68.8% of respondents to the Monash University study, for example, stated that they 'strongly support' or 'support' the use of FRT to unlock personal technology including mobile phones, followed by age verification for accessing online gambling (60.6%), verifying identity for access to financial services (57.6%), and verifying identity for access to government services (57.4%). It also found that there is less support for individual-as-operator deployments where the risks posed by the technology were perceived as disproportionately high (or the benefits disproportionately small), such as in the case of its use in apps to access online pornography (51%). This is supported by other studies, such as Krol, *et al*., (that focuses on FRT as a replacement for CAPTCHAs), which indicate the relative non-acceptability of uses for activities that do not appear to warrant the imposition of facial verification, such as booking air tickets, bidding on online auction sites, and topping up public transport cards.[56]

Table 1: Individual FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Individual	Verify Identity for applying for identity documents	Device	78.99%	Ritchie, et at.	2021	US,UK,AU
Individual	Unlock personal technology, e.g., smart phone	Device	68.8%	Andrejevic, et al.	2024	AU
Individual	Age verification for accessing online gambling	Device	60.6%	Andrejevic, et al.	2024	AU
Individual	Unlock smartphone	Device	58.9%	Kugler[57]	2019	US
Individual	Identity verification online financial services	Device	57.6%	Andrejevic, et al.	2024	AU
Individual	Identity verification for accessing govt services	Device	57.4%	Andrejevic, et al.	2024	AU
Individual	Verify Identity for access to govt websites	Device	55.72%	Ritchie, et at.	2021	US,UK,AU
Individual	Buying tickets online	Device	55%	Krol, et al.	2016	UK
Individual	Unlock smartphone	Device	54%	Ada Lovelace[58]	2019	UK
Individual	Checking in for flights online	Device	52%	Krol, et al.	2016	UK
Individual	Age verification for accessing online pornography	Device	51%	Andrejevic, et al.	2024	AU
Individual	Browsing for plane tickets	Device	45%	Krol, et al.	2016	UK
Individual	Logging into Facebook from different PC	Device	34%	Krol, et al.	2016	UK
Individual	Topping up your Oyster online	Device	31%	Krol, et al.	2016	UK
Individual	Bidding on items on eBay	Device	31%	Krol, et al.	2016	UK
Individual	Contributing to an online forum	Device	24%	Krol, et al.[59]	2016	UK

Andrejevi, *et al*. note that the relative level of public acceptance of FRT for personal device use reflects "the increasingly normalised use of the technology for opening up smartphones, and the generalised lack of adverse outcomes arising from this practice".[60] The perceived lack of adverse outcomes is likely due to the 'one-to-one' nature of this type of FRT in which the facial image of the user is compared only to the facial image of the verified user contained within the provider's database – as opposed to being compared to the stored facial images of many users. Individual operation also ranks as the most accepted operator type by Buckley & Nurse and Kostka *et al*., who cite various studies that have found that people are most likely to accept technologies, including FRT, that they are most familiar with. [61]

Expanding research results beyond one's own device to the setting of one's residence or vehicle, however, shows lower levels of acceptability. Here the technology becomes 'one-to-many' in nature whereby one's facial image is compared to that of a limited number of verified individuals (usually family members, but potentially co-tenants or neighbouring tenants, depending on the deployment). Of residence-based FRT, security-focused deployments appear to have higher levels of acceptability relative to convenience-focused deployments or deployments operated by a landlord as opposed to householders:

Table 2: Residential FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Household	Smart doorbell to identify visitors	Residential	63.9%	Kugler[62]	2019	US
Household	Smart home doorbells	Residential	58.5%	Katsanis, et al.[63]	2022	US
Landlords	Apartment buildings track who enters or leaves	Residential	51%	Pew[64]	2022	US
Household	Keyless access to front door of own home	Residential	50.8%	Andrejevic, et al.	2024	AU
Household	Monitor elderly family members in house	Residential	49.2%	Andrejevic, et al.	2024	AU
Household	Customise car settings for individual drivers	Vehicle	44.2%	Andrejevic, et al.	2024	AU
Landlords	Landlords track who enters/leaves their building	Residential	36%	Pew[65]	2019	US
Household	Customise smart home climate control settings	Residential	35.7%	Andrejevic, et al.	2024	AU
Household	Monitor children's whereabouts in house	Residential	33.3%	Andrejevic, et al.	2024	AU
Landlords	Landlords track who enters/leaves their building	Residential	31%	Katsanis, et al.	2022	US
Landlords	Enabling access to rental property	Residential	30%	Andrejevic, et al.	2020	AU

(ii) Government as Operator

A common conclusion within the literature is that public trust of government agency operation of FRT falls somewhere between operation by individuals and operation by private companies. Studies on government operation of FRT rarely distinguish between specific agencies, except for police operation, which is often treated separately. Having said this, we are able to discern the likely types of government agencies involved given the location types attributed to specific deployments, such as airports, court, hospitals, schools, roads, and public spaces. Among these deployment types there exists wide variances in public acceptability and these variances are informed by a multiplicity of acceptance factors relating to familiarity, convenience, proportionality, privacy, anonymity, security, public good, and perceptions of the ideal (and, conversely, dystopic) society.

Restricted Spaces/Entitlements

Engaging with airport security is one of the most familiar experiences of facial recognition, with Andrejevic, *et al*. noting that 36.4% of people have had personal experiences of using a face recognition terminal such as SmartGate/eGate at an airport. As is the case with the individual use of FRT to unlock smart phones, relatively high levels of familiarity correlate with relatively high levels of public acceptance. Kugler found that for non-law enforcement purposes, people in the US were generally comfortable with the use of facial recognition for identification in secure spaces, including deployments such as verifying identities at Customs (77.8%) and securing schools (72.2%), although his study notes that about a quarter of people are willing to wait in line 25 minutes to avoid using facial recognition at the airport:

Table 3: Airport FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Govt	Identity verification at passport control	Airports	77.8%	Kugler	2023	US
Govt	Identify security threat at airport (TSA)	Airports	77.6%	Kugler	2023	US
Govt	Border security	NA	76%	Andrejevic, et al.	2020	AU
Govt	Facilitate low-risk frequent travelers	Airports	71%	Unisys[66]	2014	AU
Govt	Replace passports at airports	Airports	50%	Ada Lovelace	2019	UK
Govt	Officials identify travelers at airports/stations	Airports	46%	Katsanis, et al.	2022	US

Kugler also notes that there is a difference between FRT deployed to control access to secured / limited admittance areas, such as airports and schools, and its deployment in otherwise open-access spaces, such as public parks, given the potential for ubiquitous surveillance in the case of the latter. While several studies support this, they also indicate that the level of acceptability within limited admittance areas is dependent upon the purpose of the deployment. In schools, for example, security purposes such as entry screening and identifying sex offenders within the vicinity of a school are more acceptable than the purposes of student tracking and attendance taking, which in turn are more acceptable than using FRT for monitoring student attentiveness, mood, and behaviour (refer *Table 4*). In a University of Michigan study, Galligan, *et al*. conclude that FRT in schools will likely result in exacerbating racism, normalising surveillance and eroding privacy, narrowing the definition of the "acceptable" student, commodifying data, and institutionalising inaccuracy.[67] In tertiary campuses, such concerns enjoy greater traction. US-based activist organisation Fight for the Future's "Stop Facial Recognition on Campus" campaign, for example, seeks a ban on FRT on campuses and maintains a published list of universities that "won't use", "might use", and "are using" FRT.[68]

Table 4: School FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Govt	Identify sex offenders near schools	School	80%	Andrejevic, et al.	2020	AU
Schools	Screening at public high schools	School	72.2%	Kugler	2023	US
Schools	Access to school building and grounds	School	48%	Andrejevic, et al.	2020	AU
Schools	Track student attendance	School	43%	Katsanis, et al.	2022	US
Schools	Record attendance	School	42%	Andrejevic, et al.	2020	AU
Schools	Online exam proctoring – monitoring cheating	School	40.1%	Andrejevic, et al.	2024	AU
Schools	Take student attendance	School	36.2%	Andrejevic, et al.	2024	AU
Schools	Monitor and track student whereabouts	School	32%	Andrejevic, et al.	2020	AU
Schools	Track student whereabouts in schools	School	31.6%	Andrejevic, et al.	2024	AU
Schools	Enable students to pay by face for canteen	School	29.8%	Andrejevic, et al.	2024	AU
Schools	Identify children – educational purposes	School	28%	Andrejevic, et al.	2020	AU
Schools	Monitor student attentiveness in class	School	23%	Andrejevic, et al.	2020	AU
Schools	Monitor student mood	School	19%	Andrejevic, et al.	2020	AU
Schools	Monitor students' emotions in the classroom	School	18.6%	Andrejevic, et al.	2024	AU
Schools	Monitor students' expressions and behaviour	School	6%	Ada Lovelace	2019	UK

In the case of hospitals, Katsanis, *et al*. demonstrate that patient identity verification is more acceptable in the US than other purposes, such as security and clinical deployments (refer *Table 5*). While the public places relatively high levels of trust in healthcare providers' and researchers' use of facial imaging and FRT, this does not translate into support for expanded uses in healthcare settings. Furthermore, the proliferation in the use of FRT by hospitals has occurred against a backdrop of increasing healthcare-focused cyberattacks, which has resulted in concerns over the security of biometric data collected by FRT in hospitals.[69] Katsanis, *et al*. suggest that a nuanced approach to uses of face-based data in healthcare is needed, "taking into consideration storage protection plans and the contexts of use".[70]

Table 5: Hospital FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Hospital	Identify unconscious patient in hospitals	Hospitals	80.3%	Kugler	2023	US
Hospital	Check surgery patient identities to avoid errors	Hospitals	65.9%	Katsanis, et al.[71]	2021	US
Hospital	Id non-responsive, lone, unidentified patients	Hospitals	63.4%	Katsanis, et al.	2021	US
Hospital	Verify identity of staff to access health records	Hospitals	63.1%	Katsanis, et al.	2021	US
Hospital	Faster, earlier, or better diagnosis of conditions	Hospitals	60.3%	Katsanis, et al.	2021	US
Hospital	Patient check-in at public hospitals	Hospitals	58.7%	Kugler	2023	US
Hospital	Track access/egress for potential security threats	Hospitals	57.7%	Katsanis, et al.	2021	US
Hospital	Assess threats of insurance fraud (prescriptions)	Pharmacy	52.1%	Katsanis, et al.	2021	US
Hospital	Monitor patient emotions or symptoms	Hospitals	48.4%	Katsanis, et al.	2021	US
Hospital	Linking diverse data sources for health research	Hospitals	46.5%	Katsanis, et al.	2021	US

FRT is also used by government authorities to authenticate individuals to access entitlements and to vote. By 2017, over 50 countries had adopted biometrics in elections, with many electoral authorities now using FRT to verify voter identity at polling stations – particularly where remote polling is common or where other forms of identification are unreliable. In the case of polling venues in the US and Australia, however, voter identity verification is associated with relatively lower rates of acceptability. Although governments are increasingly looking to FRT to speed up the process of accessing benefit schemes while reducing fraud, the use of FRT for this purpose in non-restricted spaces, such as retail environments, also appears to attract relatively low levels of public acceptability:[72]

Table 6: Entitlement Verification

Who	Why	Where	Accept	Study	Year	Loc
Govt	Voter identification at polling places	Voting	47%	Katsanis, et al.	2022	US
Govt	Monitor cashless welfare cards	Retail	41%	Andrejevic, et al.	2020	AU
Govt	Verify voter identity	Polls	38%	Andrejevic, et al.	2020	AU
Govt	Accessing public transport	Transit	32%	Andrejevic, et al.	2020	AU

Public Security/Safety

The value of FRT for public security and law enforcement agencies that operate it lies squarely in its ability to automate the otherwise prohibitively resource intensive process of sifting through infinite hours of CCTV footage in order to find a person of interest. The technology makes this form of investigation possible where it would have been impossible otherwise. As Kugler, Bragias, and others point out, people are concerned about the role of FRT in normalising surveillance, but they are generally accepting of the technology where its deployment serves a demonstrable *public benefit*. According to the Ada Lovelace Institute report, of the 70% of people in the UK who support the use of FRT by police in criminal investigations, 80% stated that it was because they see it as beneficial for the security of society. "The public has identified a trade-off between public benefit and the normalisation of surveillance or reduction in privacy," states the report. "In cases without a clear public benefit, people are less likely to feel comfortable with the use of facial recognition technology".[73] Among the most publicly acceptable deployments of FRT by government/police are those with the most compelling public benefit attributes: criminal investigations, terrorist identifications, and missing persons searches:

Table 7: Missing Persons

Who	Why	Where	Accept	Study	Year	Loc
Police	Search for missing persons	Open	86.06%	Ritchie, et at.	2021	US,UK,AU
Police	Identify missing child – city-wide	City	81.5%	Kugler	2023	US

Govt	Search for missing persons	N/A	80.25%	Ritchie, et at.	2021	US,UK,AU
Govt	Identify bodies of victims of war/disaster	Any	80.2%	Andrejevic, et al.	2024	AU

Table 8: Public Safety

Who	Why	Where	Accept	Study	Year	Loc
Police	Scan train station crowds to id potential terrorists	Stations	83%	LPEP[74]	2019	UK
Police	Identify potential terrorists at ticket event	Venue	82%	LPEP	2019	UK
Police	Monitor threats to society	Open	77%	Andrejevic, et al.	2020	AU
Govt	Anti-terrorism	Open	76%	Andrejevic, et al.	2020	AU
Police	Monitor crowds at large events like concerts	Venue	63%	Pew	2022	US
Govt	Monitor suspicious behaviour in public	Open	61%	Andrejevic, et al.	2020	AU
Police	Monitor crowds at protests	Open	61%	Pew	2022	US
Police	Monitor signs of aggression/antisocial behaviour	Open	59.2%	Andrejevic, et al.	2024	AU
Police	Assess security threats in public spaces	Open	59%	Pew	2019	US
Police	Assess potential security threats in public spaces	Open	54.4%	Katsanis, et al.	2022	US
Govt	Identify children (under 18) – safety purposes	N/A	48%	Andrejevic, et al.	2020	AU
Govt/Pri	Monitor mood of a crowd in real time for safety	Open	42.1%	Andrejevic, et al.	2024	AU

In the research conducted by Ritchie, *et al*., deployments relating to the investigation of crimes score generally highly in terms of public acceptability except when used to gain a conviction in the absence of other forms of evidence and when used as an investigative tool not used in court. These uses are not generally clearly regulated, “even though important decisions – such as denial of visas and plea deals – are often based substantially upon them”:[75]

Table 9: Criminal Investigations

Who	Why	Where	Accept	Study	Year	Loc
Police	Search for persons who’ve committed crime	NA	88.86%	Ritchie, et at.	2021	US, UK, AU
Police	Criminal investigations	NA	88.42%	Ritchie, et at.	2021	US, UK, AU
Govt	Conviction with other evidence in court	N/A	83.22%	Ritchie, et at.	2021	US,UK,AU
Police	Id wanted serious criminals at ticketed event	Venue	81%	LPEP	2019	UK
Police	Scan train station crowds for serious criminals	Stations	81%	LPEP	2019	UK
Govt	Search for persons who’ve committed crime	N/A	80.42%	Ritchie, et at.	2021	US,UK,AU
Police	Id homicide suspect via driver database	System	78.3%	Kugler	2023	US
Govt	Identify from CCTV images in criminal trials	System	78.37%	Ritchie, et at.	2021	US,UK,AU
Police	Criminal investigations	Open	76%	Andrejevic, et al.	2020	AU
Police	Search for persons on a watchlist	NA	75.81%	Ritchie, et at.	2021	US, UK, AU
Police	Id verification of image of criminal suspects	System	75.2%	Andrejevic, et al.	2024	AU
Police	Identify car thief via driver database	System	71.8%	Kugler	2023	US
Police	Criminal investigations	NA	70%	Ada Lovelace	2019	UK
Police	Identify car thief – city-wide	City	68.5%	Kugler	2023	US

Govt	Identify theft and fraud	Open	67%	Andrejevic, et al.	2020	AU
Govt	Identify from other images in criminal trials	System	66.86%	Ritchie, et at.	2021	US,UK,AU
Police	Identify homicide witness via driver database	System	62.9%	Kugler	2023	US
Govt	Conviction without other evidence in court	N/A	34.15%	Ritchie, et at.	2021	US,UK,AU
Govt	Investigative tool not used in court	System	34.15%	Ritchie, et at.	2021	US,UK,AU

The review research also tells us that people's comfort levels with crime-focused police FRT deployments are dependent on the nature of the crime. In short, people are more comfortable with the use of FRT for the investigation of serious crimes yet resistant to the technology being used as an investigative or monitoring tool for minor offences and antisocial behaviours:

Table 10: Minor Offences

Who	Why	Where	Accept	Study	Year	Loc
Police	Identity drivers engaged in traffic violations	Streets	65.8%	Andrejevic, et al.	2024	AU
Police	Identify wanted minor criminals at ticket event	Venue	55%	LPEP	2019	UK
Police	Identify outstanding warrants at a marathon	Event	53.9%	Kugler	2023	US
Police	Scan crowds at train stations for minor criminals	Stations	53%	LPEP	2019	UK
Govt	Traffic violations and enforcement	Open	51%	Andrejevic, et al.	2020	AU
Police	Identify wanted nuisances at ticket event	Venue	49%	LPEP	2019	UK
Police	Identify people for minor offences	Open	47%	Andrejevic, et al.	2020	AU
Police	Scan train station crowds to identify wanted nuisances	Stations	45%	LPEP	2019	UK
Police	Identify jaywalking violators for fining	Streets	41.2%	Kugler	2023	US
Govt	Identify litterers and parking violators	Open	33%	Andrejevic, et al.	2020	AU

Further, the research tells us that given the controversial nature of FRT, there are definite limits to public benefit arguments for its use by government and law enforcement. Specifically, there exists significant discomfort around surveillance deployments that are ambiguous in terms of purpose and/or scope. Kugler points out that people are often not comfortable with casual governmental facial recognition use in public spaces (refer *Table 11*). He notes that in the context of a broadly deployed facial recognition system, "a person cannot walk down a public street without having the event recorded and preserved for posterity. Anonymity in public becomes a thing of the past".[76] This type of ubiquitous surveillance erodes 'practical obscurity', or "the notion that, when information is hard or unlikely to be found, it is relatively safe".[77] Bragias and others note that the public's skepticism of new technologies being utilised by police is well documented (Bromberg *et al*., 2018, 2020; Hirose, 2017; Schwartz, 2017),[78] with specific public concerns around the erosion of privacy, undemocratic implementation, and a lack of trust.[79]

Table 11: Non-specific Surveillance

Who	Why	Where	Accept	Study	Year	Loc
Police	Police use of FRT in body worn cameras	NA	53%	Bromberg[80]	2020	US
Police	Identify political protesters	Open	47%	Andrejevic, et al.	2024	AU
Police	Day-to-day policing (trawling)	NA	41.69%	Ritchie, et at.	2021	US, UK, AU
Govt	People search irrespective of whether committed crime	N/A	37.01%	Ritchie, et at.	2021	US
Police	Automate Police work	NA	36.88%	Ritchie, et at.	2021	US, UK, AU
Police	People search irrespective of whether committed crime	NA	35.24%	Ritchie, et at.	2021	US
Govt	Track citizens	Open	34.94%	Ritchie, et at.	2021	US
Police	Track citizens	Open	32.09%	Ritchie, et at.	2021	US
Police	Monitor crowds as they walk down the street	Open	31%	Pew	2022	US
Police	Search for anyone	NA	29.61%	Ritchie, et at.	2021	US, UK, AU
Police	People search irrespective of whether committed crime	NA	27.57%	Ritchie, et at.	2021	AU
Govt/Pri	Count individual faces in a crowd	Open	28.7%	Andrejevic, et al.	2024	AU
Govt	Search for anyone	N/A	27.6%	Ritchie, et at.	2021	US,UK,AU
Govt/Pri	Track movement patterns in public spaces	Open	27.4%	Andrejevic, et al.	2024	AU
Police	People search irrespective of whether committed crime	NA	26.02%	Ritchie, et at.	2021	UK
Govt	Track citizens	Open	25.8%	Ritchie, et at.	2021	US,UK,AU
Police	Track citizens	NA	25.31%	Ritchie, et at.	2021	US, UK, AU
Govt	Track citizens	Open	23.58%	Ritchie, et at.	2021	UK
Police	Track citizens	NA	23.67%	Ritchie, et at.	2021	UK
Govt	People search irrespective of whether committed crime	N/A	23.38%	Ritchie, et at.	2021	AU
Govt	People search irrespective of whether committed crime	N/A	22.40%	Ritchie, et at.	2021	UK
Police	Search for persons not on a watchlist	NA	22.13%	Ritchie, et at.	2021	US, UK, AU
Police	Track citizens	NA	20.18%	Ritchie, et at.	2021	AU
Govt	Track citizens	Open	18.88%	Ritchie, et at.	2021	AU

In the UK, the Ada Lovelace Institute study revealed that 55% of people think that government should limit police use of FRT via regulation to specific circumstances. The study further found that the public supports companies voluntarily pausing sales of facial recognition technology to police (50%) and schools (70%) to allow for further public consultation.[81] A January 2024 letter by the UK Parliament Justice and Home Affairs Committee to the UK Home Secretary went so far as stating that FRT's use by police is "lacking in legal foundation". The Committee accepted that live facial recognition may be a valuable tool for police forces in apprehending criminals, but stated it is deeply concerned that its use is being expanded without proper scrutiny and accountability. "To us it seems the fact that the technology is regarded as controversial means that continued public support cannot be taken for granted," its letter stated.[82] In the US, amidst widespread protests against police brutality in June 2020, IBM, Microsoft, and Amazon announced that they would deny police departments access to their FRT services, advocating that governments should enact stricter regulations to govern its use (Magid, 2020). Three cities in California and two cities in Massachusetts have voted to ban the use of FRT by city departments and local police,[83] several countries have banned police use of FRT, and, as mentioned earlier, New Zealand Police policy has just recently placed a stop on its deployment of Live FRT.[84] "If there's limited social licence [for FRT], then not using it is a sensible decision," notes James Sweetland. "It's a valuable tool, but one that remains controversial and is best applied where public trust won't be undermined by its use... yet, as FR becomes more common in Western policing, perhaps that public trust calculation will change".[85]

(iii) Private Business as Operator

As mixed as public support for government operation of FRT may be, it is generally greater than existing levels of support for operation of FRT by the private sector. According to Smith (2019), a Pew Research Center survey of 4,272 American adults in June 2019 found that a majority (56%) trusted law enforcement agencies to use FRT responsibly when assessing security threats in public spaces, while a significantly smaller percent of them trusted technology companies (36%), companies tracking employee attendance (30%), or advertisers (18%). According to the research, people are less comfortable with the use of FRT when they perceive it is being used for commercial benefit. In the Kosta *et al*. study, when asked about the extent to which respondents would accept FRT when managed by central or local governments, private companies, or public–private partnerships (PPPs), the acceptance for FRT use by private enterprises is only 15% in Germany, 17% in China, 20% in the United Kingdom, and 30% in the United States. As is the case with government/police use of FRT, private sector operation of FRT is the subject of restrictions in some jurisdictions.[86]

Retail

According to the NZ Privacy Commissioner survey results, 49% of respondents stated that they were concerned or very concerned about the use of facial recognition technology in retail stores to identify individuals. A total of 22% were neutral on the topic, 25% were either not concerned or not really concerned, and 11% were unsure, suggesting low public acceptability for FRT deployments in retail contexts. Those aged 30-44 were more likely to express concern about retail use of facial recognition (55%), and women and Maori were more likely to say they were concerned. In Australia, according to Andrejevi *et al*., 54.4% of respondents 'strongly support' or 'support' use of FRT by retail outlets and shops for identifying shoplifters and anti-social patrons (although, importantly, this study appears not to have indicated that FRT included live deployments).

The majority did not support its use for tracking and targeting shoppers, and there was a strong sense facial recognition technology should not be used for commercial benefit. According to the Ada Lovelace Institute study, most people (70%) are uncomfortable with the use of FRT in retail because they do not trust companies to use the technology ethically (63%).[87] Results from across the reviewed research indicates that in retail contexts the public is more accepting of FRT to identify shoplifters, antisocial patrons, and fraud than it is of other use cases, such as loyalty programs, advertising, payments, and the tracking of customer behaviour:

Table 12: Retail FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Private	Identity verification for weapons purchases	Retail	70%	Andrejevic, et al.	2020	AU
Private	Detect known shoplifters	Retail	58.9%	Kugler	2023	US
Private	Identify individuals banned from store	Retail	54.8%	Katsanis, et al.	2022	US
Private	Identify shoplifters and antisocial patrons	Retail	54.4%	Andrejevic, et al.	2024	AU
Private	Confirming credit card account holders at checkout	Retail	53%	Pew	2022	US
Private	Age verification for alcohol/tobacco	Retail	46%	Andrejevic, et al.	2020	AU
Private	Prevent theft/fraud in stores/malls	Retail	44%	Andrejevic, et al.	2020	AU
Private	Coffee shop customer loyalty (replace cards)	Retail	39.3%	Katsanis, et al.	2022	US
Private	Track customer movement for advertising	Retail	36.8%	Katsanis, et al.	2022	US
Private	Blacklist people who've behaved antisocially	Retail	36.71%	Ritchie, et at.	2021	US,UK,AU
Private	Administer customer loyalty program (replace cards)	Retail	35.2%	Kugler	2019	US
Private	Share data to blacklist people	Retail	32.21%	Ritchie, et at.	2021	US,UK,AU
Private	Track people behaving antisocially	Retail	31.31%	Ritchie, et at.	2021	US,UK,AU
Private	Enable customers to 'pay by face'	Retail	31.3%	Andrejevic, et al.	2024	AU
Private	As a means of paying	Retail	31%	Andrejevic, et al.	2020	AU
Private	Identify customers in loyalty programs	Retail	26%	Katsanis, et al.	2022	US
Private	Track shoppers and serve targeted advertisements	Retail	25.8%	Kugler	2023	US
Private	Identify individuals	Retail	25%	OPC	2024	NZ
Private	Identify and track shoppers	Retail	23%	Andrejevic, et al.	2020	AU
Private	Customise advertising for shoppers	Retail	21%	Andrejevic, et al.	2020	AU
Private	Collect demographic information on shoppers	Retail	19.4%	Andrejevic, et al.	2024	AU
Private	Verify age for alcohol purchases in supermarkets	Retail	17%	Ada Lovelace	2019	UK
Private	Customise advertising to individual shoppers	Retail	15.7%	Andrejevic, et al.	2024	AU
Private	Monitor customer moods	Retail	14.2%	Andrejevic, et al.	2024	AU
Private	Identify children (under 18) – marketing purposes	Retail	12%	Andrejevic, et al.	2020	AU
Private	Shopper demographic information	Retail	9.4%	OPC	2024	NZ
Private	Shopper behaviour tracking in supermarkets	Retail	7%	Ada Lovelace	2019	UK

Workplaces

Workplaces are spaces in which there exist lower still levels of public acceptability of FRT. Similar to retail deployments, security-related deployments attract greater acceptability than uses relating to employee location and behaviour tracking:

Table 13: Workplace FRT deployments

Who	Why	Where	Accept	Study	Year	Loc
Private	Access to secure locations	Workplace	55%	Andrejevic, et al.	2020	AU
Govt/Priv	Id thieves, security (also attendance/ performance)	Workplace	54%	Rainie, Duggan	2016	US
Govt/Priv	Id thieves, security only	Workplace	48%	Doberstein, et al.	2022	CAN
Private	Clock in and out of work	Workplace	43%	Andrejevic, et al.	2020	AU
Govt/Priv	Id thieves, security (also attendance/ performance)	Workplace	41%	Doberstein, et al.[88]	2022	CAN
Private	Track employee attendance	Workplace	35%	Katsanis, et al.	2022	US
Private	Screen job applicants	Workplace	32%	Andrejevic, et al.	2020	AU
Private	Automatically tracking attendance of employees	Workplace	30%	Pew	2022	US
Govt/Priv	Purposes other than security	Workplace	27%	Doberstein, et al.	2022	CAN
Private	Monitor behaviours and practices	Workplace	23%	Andrejevic, et al.	2020	AU
Private	Monitor employee whereabouts	Workplace	21%	Andrejevic, et al.	2020	AU
Private	Track worker location	Workplace	18.1%	Andrejevic, et al.	2024	AU
Private	Monitor productivity of employees	Workplace	16.4%	Andrejevic, et al.	2024	AU
Private	Monitor employee mood	Workplace	16%	Andrejevic, et al.	2020	AU
Private	Monitor worker emotion during the working day	Workplace	12.9%	Andrejevic, et al.	2024	AU
Private	Monitor personality traits / mood of job candidates	Workplace	4%	Ada Lovelace	2019	UK

Gambling and age-restricted venues

Private sector deployment of FRT (and specifically live FRT) is relatively widespread in the casino and gaming sector. Large casinos have been enthusiastic ‘early adopters’ of facial recognition well before the technology was considered reliable enough to be used elsewhere in society.[89] It is seen as an affordable and reliable means of overcoming the inconsistencies of manually enacted identification and verification processes, particularly in relation to self-reported problem gamblers. The South Australian Government, for example, requires venues with 30 or more gaming machines to install FRT for identifying barred patrons.[90] While the gambling industry and some regulators have been sold on the benefits of FRT, some studies point to its ineffectiveness. Selwyn, *et al.*, for example, note that FRT does not better address the core issues underpinning problem gambling, nor does it substantially improve conditions that support people with problem gambling. There are also inconsistencies with how the technology is applied, as well as inefficiencies and uncertainties.[91] The Alliance for Gambling Reform[92] and Foundation for Alcohol Research and Education (FARE) have advocated for a moratorium on FRT use in gambling venues across Australia due to alarming warnings from human rights experts that such technology violates privacy laws.[93] As with the deployment of FRT in other contexts, the lowest levels of acceptability in gaming contexts relate to customer loyalty/marketing and behaviour monitoring uses:

Table 14: Gambling and age-restricted spaces

Who	Why	Where	Accept	Study	Year	Loc
Private	Age verification for accessing gambling venues	Casinos	68%	Andrejevic, et al.	2024	AU
Private	Prevent entry of self-excluded gamblers at casinos	Casinos	64.4%	Andrejevic, et al.	2024	AU
Private	Identify performer stalkers	Venues	60%	Kugler[94]	2023	US
Private	Screen dating app users for DV record	Online	56%	Andrejevic, et al.	2020	AU
Private	Identify VIP customers at the door	Casinos	42.7%	Andrejevic, et al.	2024	AU
Private	Cashless payment for gambling/alcohol at venues	Venues	23.8%	Andrejevic, et al.	2024	AU
Private	Monitor the mood in a club to adjust the music	Venues	22%	Andrejevic, et al.	2024	AU

In addition to the deployment types discussed above, there are other private sector deployments of FRT captured in various public acceptability studies, some of which are featured in *Table 15*. These generally attract relatively low levels of public acceptability, and are often associated with misuse. In one example, an application that allows users to match a person's face photo with social media profiles to obtain a person's contact information was used by moral crusaders to find pornographic actresses' social media pages and send scandalous messages and images to their relatives and friends.[95] As with other deployment types, deployments relating to advertising and deployments lacking a specific purpose attracted lower levels of public acceptability than those relating to security:

Table 15: Other deployments

Who	Why	Where	Accept	Study	Year	Loc
Private	Identity verification at ATMs	ATMs	50%	Andrejevic, et al.	2020	AU
Private	Identify unknown persons in uploaded photos	Online	43%	Kugler	2019	US
Private	Internet based people search products	Online	37.7%	Katsanis, et al.	2022	US
Private	Homeowner Assoc. track people on streets	Streets	36.7%	Katsanis, et al.	2022	US
Private	Find photos of users on other companies' websites	Online	32.8%	Kugler	2019	US
Private	Homeowners' association tracking people movement	Streets	31.9%	Kugler	2019	US
Private	Homeowner association monitoring own streets	Streets	31.9%	Kugler	2023	US
Private	Link profiles across social media sites	Online	30.9%	Kugler	2019	US

Private	Track people's locations using publicly uploaded photos	Online	28.7%	Kugler	2019	US
Private	Track citizens	Open	28.15%	Ritchie, et at.	2021	US
Private	Comb social media to track celebrities' photos/ locations	Online	26.2%	Kugler	2019	US
Private	Monitor responses to public advert displays	Open	23%	Katsanis, et al.	2022	US
Private	Social media sites auto id'ing people in photos	Online	19%	Pew	2022	US
Private	Track citizens	Open	17.21%	Ritchie, et at.	2021	US,UK,AU
Private	Monitor responses to public advert displays	Open	15%	Pew	2019	US
Private	Track citizens	Open	13.10%	Ritchie, et at.	2021	UK
Private	Track citizens	Open	10.39%	Ritchie, et at.	2021	AU

A glaring problematic in the data overall is, of course, the lack of it in relation to New Zealand. This is significant given that the data – even between politically and socially proximate countries (such as the UK, US, and Australia) does differ and that New Zealand's bicultural identity, for example, means that such issues as Maori data sovereignty hold critical importance locally. Nevertheless, the approximately 200 data points provided by the collated US, UK, and Australian research provide us with a clear picture of deployment specific FRT public acceptability among those jurisdictions, which are of indicative value for acceptability modelling in the New Zealand context.

"It's difficult to gauge how consumers in New Zealand feel about the use of facial recognition by retailers because no-one has asked them," wrote Ruairi O'Shea in a November 2022 Consumer NZ article. As it turns out, neither has the question been asked of New Zealanders generally. To date, there has been no empirical study of public attitudes in New Zealand around FRT deployments and their acceptability. Despite noting this, an extensive New Zealand Law Foundation report on FRT in New Zealand published in 2020 comments that the views of the public constitute a potential constraint on the expansion of surveillance through FRT.[96] Indeed, in a 2021 article promoting the report, co-author Associate Professor Nessa Lynch of Victoria University of Wellington comments that the "role of public opinion on matters like this is massive". The report raises the relevance of social licence, and quotes the definition of it offered by Gulliver, *et al*. for the New Zealand data context: "… societal acceptance that a practice that lies outside general norms may be performed by a certain agent, on certain terms". It's a relevance not lost on NZ Police, with Police Technology Assurance adviser Dr Andrew Chen commenting during a July 2024 webinar that given FRT's controversial nature, the overriding principle for Police "is maintaining public trust and policing by consent".[97] A clearly established relationship exists between social acceptability and social licence, and this is relevant to FRT (and biometric technologies generally), yet the major research and policy documents produced in New Zealand to date – including those by the Office of the Privacy Commissioner, NZ Police, research institutions, and others – have not incorporated empirical acceptability data into their findings.

An FRT Public Acceptability Model

Of government uses of FRT, Kugler argues that given the norms of democratic accountability, public attitudes are likely relevant to where the line should be drawn between permissible and impermissible uses. As the preceding paragraph notes, there is no reason why this statement is any less relevant in relation to uses of FRT beyond government. Laufs and Borrion note that "although social acceptability and the view of the general public can hinder or even fully stop the deployment and use of new crime prevention and detection tools, the threshold for this is often arbitrary and rarely follows an evidence base". What is a reasonable quorum when it comes to determining a minimum level of public acceptance justifying the deployment of an FRT system? Is a simple majority enough, or would something resembling a referendum-type majority be more appropriate? What is an appropriate majority in comparison to those who are unaccepting, those who are undecided, and those who are not adequately knowledgeable to offer a position? What weighting should acceptability considerations be given, and who decides? Indeed, thresholds, even where they may be established, are culturally and socially constituted (reflecting political systems and social values) historically contingent (reflecting technological maturity and societies' evolving relationships with technologies), and unpredictably reactive (in terms of nature and duration) to critical events and environmental sudden shifts (such as 9/11, COVID-19, or a sharp spike in crime). However, as the preceding review of the research demonstrates, despite the absence of an established FRT public acceptability threshold, there nevertheless exist distinct patterns influenced by deployment factors (who, why, where, and how). Within a specific societal and temporal context, these can provide us with the basis upon which to indicatively map specific deployments within a matrix of acceptability.

To form the axes of this matrix, we can look to TAM and the various trade-off approaches that present acceptability factors as a series of perceived risks and benefits. They provide us with the basis for a model in which FRT acceptability may be represented as a trade-off between risks and rewards or, more specifically 'perceived risk' and 'reward proximity'.

Reward Proximity and Perceived Risk

Reward proximity is a concept that attempts to reflect the findings of the reviewed research that suggest a distinct pattern to the variations in perceived reward as we cycle through the various examples of individual, government, and private sector FRT deployments. In the case of individual device-based operation of FRT, we see that the individual is both 'operator' and subject, and that rewards – such as ease of use, convenience, and usefulness – are experienced immediately and personally. These rewards are in close – literally tangible – proximity to the individual. In the case of private company operation of FRT, such as customer tracking in a retail store, we see that the individual is merely a subject (they are subjected to having their facial biometric collected) and that the operator, motivated largely by commercial self-interest, is the predominant beneficiary of the operation of FRT. In this case, individuals are distanced from any rewards gained through the operation of the technology. However, if the retailer is operating FRT in order only to identify known shoplifters, then it could be argued that individuals may perceive at least some indirect benefit from less in-store criminality. Finally, in the case of government operation of FRT, such as in the conduct of a criminal investigation, we see that individuals are likely to perceive a public benefit from its use and that they are rewarded indirectly by it in terms of a more effective criminal justice system and, ultimately, a safer community. In the case of FRT at airport passport control, it could be argued that individuals perceive both direct benefit (faster processing through customs) and indirect benefit (society protected through effective border security).

Reward proximity allows us to conceptualise the perceived benefits of FRT operation from the perspective of individuals as being of:

- *Direct benefit:* personal benefit to individuals whose facial images are being captured. Examples of these benefits may include perceived usefulness, perceived enjoyment, perceived ease of use, efficiency, convenience, improved personal security.
- *Indirect benefit:* individuals whose facial images are being captured perceive a social or public benefit. Examples of these benefits may include improved public safety (safer communities), positive social outcomes (for example, restricting venue access to problem gamblers and underage drinkers) or national security (protection from national security threats or better protected government premises); or
- *Ex parte benefit:* where individuals whose facial images are being captured perceive that the benefits appear to reside largely with another party (the operator) who is acting predominantly in self-interest. Examples of these benefits may include improved premise/workplace security, business efficiencies and cost savings, and increased profit.

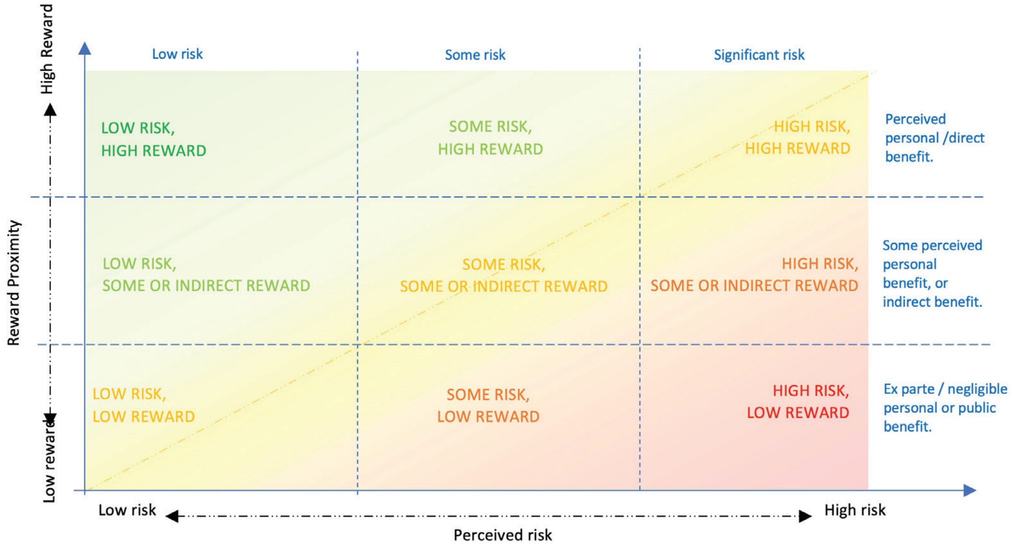
Direct, indirect, and *ex parte* benefit thus can be thought of in terms of inhabiting varying levels of proximity to the individual, with direct benefit being the most tangible and *ex parte* benefit being the most distant.

Perceived risk refers to the varied risks attributed by the public to specific FRT deployments. The reviewed research indicates that certain groups within society are more exposed (vulnerable) than others to the risks posed by the technology, including algorithmic inaccuracies/biases that can lead to discriminatory false identification and potential embarrassment, trauma, mistreatment, and prejudicial enforcement outcomes. Individuals are perhaps more uniformly exposed to certain other risks, such as the potential for undeclared use or misuse, either by the operator or by a malicious third party (such as a data breach), which can result in personal data harvesting for unauthorised or illicit use (such as identity theft). The potential for ubiquitous surveillance posed by FRT poses present and future risks to society itself, such as the wholesale loss of citizen anonymity and behavioural freedoms resulting from the 'chilling effect' of omnipresent surveillance. Lastly, there exist the risks – unknowns or uncertainties – posed by the current lack of public awareness and understanding of the technology and the absence of legislated restrictions on its use.

Unlike the risk-return trade-off in economics, SOST acceptance is not a zero-sum trade-off between the two. Higher levels of risk are not necessarily associated with higher levels of reward, and achieving less risk does not require a corresponding loss of reward. An FRT deployment can be perceived as high risk and low reward, and vice versa. Eposti & Gomez, for example, found that although around half of the population see SOST acceptance as a trade-off between security and liberty, half did not, with many seeing the tech as highly intrusive yet ineffective, or not intrusive yet very effective. An individual does not necessarily trade risk for reward, as they are distinct considerations. Ultimately, however, the level of public acceptability of a specific deployment is likely the result of the aggregate perceived downsides balanced against the expected upsides. It is assumed that the risk/reward calculus is consistent with rational choice theory's premise that decisions made by individual actors collectively produce aggregate social behaviour.

Based on the above, *Figure 1* (overleaf) is offered as a simple model for understanding the indicative public acceptability of various FRT deployments. In this model, *risk* forms the x-axis and *reward* forms the y-axis. The risk spectrum is graduated according to three descriptors: Low Risk, Some Risk, and Significant Risk, and the reward spectrum is also graduated according to three descriptors: Direct Benefit, Indirect Benefit, and *Ex parte* Benefit. The intersecting grades of risk and reward form a matrix made up of segments that each correspond to distinct risk/reward combinations extending from low risk/high reward in the top left to high risk/low reward in the bottom right. Extending from low risk/low reward in the bottom left to high risk/high reward in the top right is a trade-off line along which risk and reward are at – or close to – equilibrium.

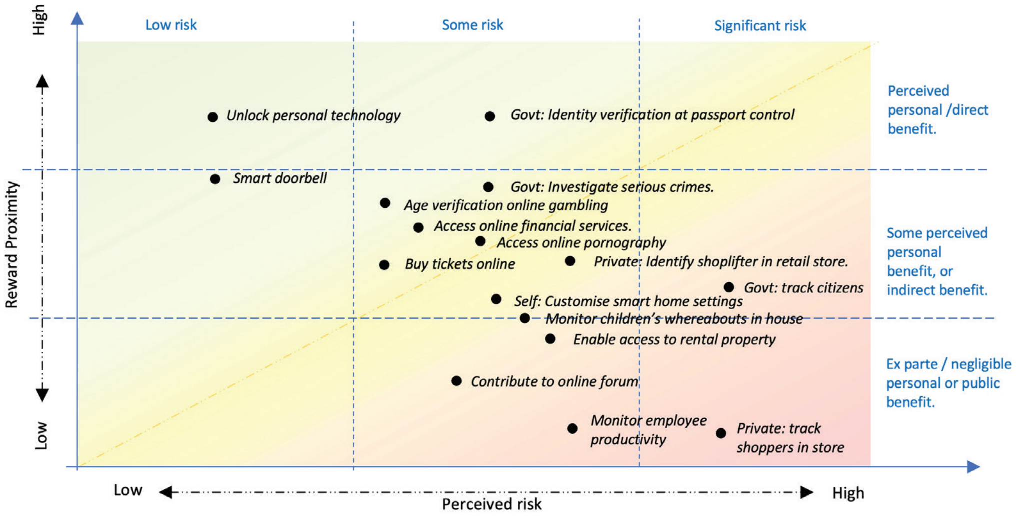
Figure 1: FRT Public Acceptability Model


High Reward
Reward Proximity
Low reward
Low risk
Some risk
Significant risk
LOW RISK, HIGH REWARD
SOME RISK, HIGH REWARD
HIGH RISK, HIGH REWARD
Perceived personal /direct benefit.
LOW RISK, SOME OR INDIRECT REWARD
SOME RISK, SOME OR INDIRECT REWARD
HIGH RISK, SOME OR INDIRECT REWARD
Some perceived personal benefit, or indirect benefit.
LOW RISK, LOW REWARD
SOME RISK, LOW REWARD
HIGH RISK, LOW REWARD
Ex parte / negligible personal or public benefit.
Low risk
High risk
Perceived risk

Various examples of FRT deployments may be plotted in the matrix based on an approximation of the level of risk and reward attributed to them by the reviewed 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 level one may have that it would meet with unacceptability. For multiple plotted deployments on a graph to be comparable, they should all relate to a common society and time period. The model is intended to provide organisations operating FRT and the security consultants, integrators, and vendors advising them with a template for the plotting of existing and intended FRT deployments that maps their public acceptability relative to other deployments and informed by the existing FRT public acceptability data. As an example, *Figure 2* plots the approximate comparative public acceptability of selected individual, government, and private FRT deployments. Using this model, FRT operators and their security industry advisers can more effectively consider the appropriateness of their intended FRT deployments and the extent to which they may expose the operator to potential enterprise risks, such as public controversy, reputational risk, and related costs.

Figure 2: FRT Public Acceptability Model – selected deployments

[next page]



Conclusion

Emerging 'smart' technologies within contemporary SOSTs, such as biometric analytics and artificial intelligence, are neither inherently 'good' or 'bad', but they are powerful and currently unwieldy. They are unwieldy because the speed at which they are being developed and becoming more powerful typically outstrips the speed of public awareness, political debate, and legislative developments needed to define limits to their power in line with societal conceptions of 'good' and 'bad'. Left unchecked, the power that FRT can wield poses an unprecedented threat to privacy, individual freedoms, and the character of our societies. Conversely, with the right safeguards, the technology can deliver untold benefits for public safety and security, identity management, and efficiencies in achieving these.

Given the connection between public acceptability and social licence in relation to SOSTs, this paper recommends that empirical research be undertaken into the public acceptability of FRT deployments among New Zealanders. Understanding how various FRT deployment scenarios are perceived by New Zealanders would be useful in identifying how local perceptions differ from those in the existing international research (such as the US, UK, and Australia), and in establishing an evidence basis for discussing and developing legislative and policy-driven safeguards. The biennial privacy survey of New Zealanders by the Office of the Privacy Commissioner (OPC) goes a little way in this regard, but as a survey on privacy concerns that fall within the OPC's Privacy

Act remit it affords limited attention to FRT specifically. The recent public consultation conducted by the OPC on an exposure draft of a biometrics code of practice is another recent example of eliciting public perceptions, but again it is not FRT deployment-specific, and nor does it engage directly with issues of acceptability.[98] In the absence of local research on FRT public acceptability, the academics who inform policy, experts and lobbyists who seek to influence it, and officials who formulate it, are left to draw their conclusions largely from foreign data and foreign guardrail precedents. They do so without first having empirically established either the existence of social licence for it in New Zealand or the range of scenarios that social licence might cover.

Even when legislated safeguards and associated guidance on FRT are ultimately enacted, in addition to ensuring their CCTV and/or privacy policies are consistent with it, organisations operating FRT will be faced with the challenges of interpreting and applying it to specific deployment scenarios. This may include factoring it into outputs such as feasibility studies, internal business cases, systems specifications, or security system designs, as well as the completion of prescribed documents, such as Privacy Impact Assessments. As ought to be the case currently, organisations looking to operate FRT will look to relevant practitioners, such as security, risk, and privacy advisers, to provide advice as to the appropriateness of specific FRT deployment scenarios. Given the professional knowledge and experience they are expected to possess, licensed security consultants are arguably the most aptly placed of all parties within the SOST supply chain to provide sound advice relating to the appropriateness and acceptability of proposed FRT deployments to their clients.

Many security practitioners are no doubt already doing just that, but they are doing so in unchartered territory with little to guide them, and in the meantime controversial FRT deployments continue to attract adverse media attention and reputational outcomes. This paper and its proposed FRT Public Acceptability Model joins a limited body of barely established scholarship intended to assist practitioners in this regard. It also welcomes the prospect of greater political involvement in defining the responsible use of FRT and its place in the future of our societies.

[1] “Foodstuffs North Island begins trialling facial recognition in select stores as part of its commitment to keep teams and customers safe by keeping previous offenders out”, Foodstuffs North Island Limited, 08 February 2024. https://www.foodstuffs.co.nz/news-room/2024/Foodstuffs-North-Island-begins-trialling-facial-recognition-in-select-stores. According to *Facial Recognition Technology Trial – Privacy Impact Assessment Report*, Foodstuffs North Island, February 2024. P. 8., Persons of Interest (POIs) include individuals that have “engaged in Harmful Behaviour” by stealing or attempting to steal from the store; damaging store product(s) and/or property; assaulting (physically or verbally), or behaving in a violent, aggressive, threatening or abusive manner towards, staff and/or other customers; or re-entered the Store in breach of their trespass notice; or their accomplices.

[2] Ruairi O’Shea, “Facial recognition at 29 Foodstuffs North Island stores”, Consumer NZ, 23 November 2022. https://www.consumer.org.nz/articles/facial-recognition-at-29-foodstuffs-north-island-stores

[3] George Block, “The quiet creep of facial recognition systems into New Zealand life”, *Stuff,* 01 January 2020. https://www.stuff.co.nz/technology/118202977/the-quiet-creep-of-facial-recognition-systems-into-new-zealand-life; George Block, “Rise of AI: NZ supermarkets using facial recognition”, *Otago Daily Times*, 14 May 2018. https://www.odt.co.nz/news/national/rise-ai-nz-supermarkets-using-facial-recognition

[4] Sandra Conchie, “Supermarket facial recognition trial: Rotorua mother’s ‘discrimination’ ordeal”, *Rotorua Daily Post* / *New Zealand Herald*, 13 April 2024. https://www.nzherald.co.nz/nz/supermarket-facial-recognition-trial-rotorua-mothers-discrimination-ordeal/IK4ZEJHLQVFRLMDE6LX4AR57PE/

[5] Mark Rickerby, “Supermarket facial recognition failure: why automated systems must put the human factor first”, *The Conversation*, 22 April 2024. https://theconversation.com/supermarket-facial-recognition-failure-why-automated-systems-must-put-the-human-factor-first-228284. Republished by *1 News*, 23 April 2024. https://www.1news.co.nz/2024/04/23/supermarket-facial-recognition-failure-how-to-avoid-this-happening-again/

[6] (Trenton W. Ford, “It’s time to address facial recognition, the most troubling law enforcement AI tool”, *Bulletin of the Atomic Scientists*, 10 November 2021, https://thebulletin.org/2021/11/its-time-to-address-facial-recognition-the-most-troubling-law-enforcement-ai-tool/). For more detail, see Raposo, V.L. “When facial recognition does not ‘recognise’: erroneous identifications and resulting liabilities”, *AI & Society*, 39, 1857–1869 (2024). https://doi.org/10.1007/s00146-023-01634-z

[7] Jon Duffy, “Facial recognition: The supermarkets are watching you”, Consumer NZ, 05 March 2024. https://www.consumer.org.nz/articles/facial-recognition-the-supermarkets-are-watching-you

[8] Sharon Masige, “With Woolworths staff using body worn cameras, what are the legal considerations? “, *Human Resources Director* (HRD), 09 May 2024. https://www.hcamag.com/nz/specialisation/hr-technology/with-woolworths-staff-using-body-worn-cameras-what-are-the-legal-considerations/488421

[9] *Woolworths New Zealand reaffirms commitment to customer privacy and data security in response to recent misinformation*, Woolworths, 2024. https://www.woolworths.co.nz/info/news-and-media-releases/2024/woolworths-nz-reaffirms-commitment-to-customer-privacy

[10] Amy Hall, “Bunnings denies reintroducing facial recognition technology amid privacy investigation”, *SBS News*, 14 July 2023. https://www.sbs.com.au/news/article/bunnings-denies-reintroducing-facial-recognition-technology-amid-privacy-investigation/11m26l1of

[11] Jeremy Nadel, “Bunnings and Kmart facial recognition probe set to finish by July, *IT News*, 14 February 2023. https://www.itnews.com.au/news/bunnings-and-kmart-facial-recognition-probe-set-to-finish-by-july-590881

[12] “OAIC finds against 7-Eleven over facial recognition”, Office of the Australian Information Commissioner, 14 October 2021. https://www.oaic.gov.au/newsroom/oaic-finds-against-7-eleven-over-facial-recognition

[13] Mackenzie Smith, “Police trialled facial recognition tech without clearance”, *Radio NZ*, 13 May 2020. https://www.rnz.co.nz/news/national/416483/police-trialled-facial-recognition-tech-without-clearance

[14] “Police release findings from independent expert review of Facial Recognition Technology”, New Zealand Police, 09 December 2021. https://www.police.govt.nz/news/release/police-release-findings-independent-expert-review-facial-recognition-technology

15 Phil Pennington, “NZ Police finally has facial recognition policy – but is it strict enough?”, *RNZ*, 20 August 2024. https://www.rnz.co.nz/news/media-technology/525642/nz-police-finally-has-facial-recognition-policy-but-is-it-strict-enough

16 James Vyver, “Australian retail giants and police using artificial intelligence software Auror to catch repeat shoplifters”, *ABC News*, 10 June 2023. https://www.abc.net.au/news/2023-06-10/retail-stores-using-ai-auror-to-catch-shoplifters/102452744

17 Cam Wilson, “AFP suspends use of controversial surveillance tech found in Woolworths, Bunnings”, *Crikey*, 17 July 2023. https://www.crikey.com.au/2023/07/17/afp-auror-surveillance-tech/

18 Carey Doberstein, Etienne Charbonneau, Genevieve Morin, and Sarah Despatie, “Measuring the Acceptability of Facial Recognition-Enabled Work Surveillance Cameras in the Public and Private Sector”, *Public Performance & Management Review*, 2022, Vol 45, No 1. P.202. https://doi.org/10.1080/15309576.2021.1931374

19 Laufs and Borrion, loc cit. p.198.

20 Paul Cullen, “How Do Casinos Use Facial Recognition Technology?”, *Techopedia*, 18 July 2024. https://www.techopedia.com/gambling-guides/casino-facial-recognition-technology

21 Shoshana Zuboff, *The Age of Surveillance Capitalism*, London, Profile Books, 2019. A 18 August 2024 internet search by the author of the term “facial recognition casino gambler” returned several matches featuring FRT vendor websites promoting the value of FRT’s dual-use in casinos.

22 *Inquiry into Cashless Gaming in the ACT ANSWER TO QUESTION TAKEN ON NOTICE* [by the ACT Council of Social Service], Legislative Assembly for the Australian Capital Territory, Standing Committee on Justice and Community Safety, 27 March 2024. https://www.parliament.act.gov.au/__data/assets/pdf_file/0003/2436258/JACS-QTON-007-ACTCOSS-Facial-recognition-Braddock.pdf

23 *Facial Recognition Technology Trial – Privacy Impact Assessment Report*, op cit. P.6.

24 *Research on Privacy Concerns and Data Sharing*, April 2024. Prepared for the Privacy Commissioner. https://policycommons.net/artifacts/12602776/research-on-privacy-concerns-and-data-sharing/13504205/

25 *Privacy Week 2024: New survey reveals New Zealanders privacy concerns*, Office of the Privacy Commissioner, 13 May 2024. https://www.privacy.org.nz/publications/statements-media-releases/privacy-week-2024-new-survey-reveals-new-zealanders-privacy-concerns/

26 Andrejevic M, Selwyn N, Gu X, Smith G, O’Malley P, O’Neill C (2024), *Australian Public Attitudes to Facial Recognition Technology*, Monash University, Clayton. https://drive.google.com/file/d/1Teo8eOYoAucdb7hb2CUakfVElauQizVE/view

27 *Beyond face value: public attitudes to facial recognition technology*, London, Ada Lovelace Institute, September 2019. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

28 *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, Pew Research Center, September 2019. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf

29 Andrejevic M, et al. Loc cit.

30 Ritchie KL, Cartledge C, Growns B, Yan A, Wang Y, Guo K, et al. (2021), “Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world”, *PLoS ONE*, 16(10): e0258241. https://doi.org/10.1371/journal.pone.0258241

31 Genia Kostka, Lea Steinacker, Miriam Meckel, “Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States”, *Public Understanding of Science*, 2021, Vol. 30(6). p.679. DOI: 10.1177/09636625211001555.

32 Fred Davis, “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”, *MIS Quarterly*, Vol. 13, No. 3, September 1989, University of Minnesota. https://doi.org/10.2307/249008

33 Genia Kostka, loc cit.

34 Tao Liu, Bijiao Yang, Yanan Geng, Sumin Du, “Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology”, *Frontiers in Psychology*, Vol 12, December 2021. https://doi.org/10.3389/fpsyg.2021.809736

35 Bahareh Nakisa, Fatemeh Ansarizadeh, Prem Oommen, Rahul Kumar, “Using an extended technology acceptance model to investigate facial authentication”, *Telematics and Informatics Reports*, Volume 12, December 2023. https://doi.org/10.1016/j.teler.2023.100099

[36] Ibid. p.9.

[37] Patrick Ajibade, “Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches”, *Library Philosophy and Practice*, Summer 2018.

[38] Vincenzo Pavone, Sara Degli-Esposti, Elvira Santiago, *Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*, SurPRISE Project, 2015.

[39] See: Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York: Pantheon, 1977.

[40] Ibid. p.4.

[41] Julian Laufs and Hervé Borrion, “Technological innovation in policing and crime prevention: Practitioner perspectives from London”, *International Journal of Police Science & Management*, 2022, Vol. 24(2) 190–209.

[42] Ibid. p.192.

[43] Mark Andrejevic, Chris O’Neill, Gavin Smith, Neil Selwyn, Xin Gu, “Granular biopolitics: Facial recognition, pandemics and the securitization of circulation”, *New Media & Society*, 2024, Vol. 26(3) 1204-1226. https://doi.org/10.1177/14614448231201638

[44] Barry Buzan, Ole Wæver, Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner, 1998.

[45] Mark Andrejevic, Chris O’Neill, Gavin Smith, Neil Selwyn, Xin Gu, loc it. P.1212. See also Athina Ioannou, Iis Tussyadiah, “Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours”, Technology in Society, Volume 67, November 2021. https://doi.org/10.1016/j.techsoc.2021.101774

[46] Misse Wester, Johan Giesecke, “Accepting surveillance – An increased sense of security after terror strikes?”, *Safety Science*, Vol 120, December 2019, Pages 383-387. https://doi.org/10.1016/j.ssci.2019.07.013

[47] Ibid. P.387.

[48] Mark Andrejevic, et al., Loc cit. P.11.

[49] Ankita Guleria, Kewal Krishan, Tanuj Kanchan, “Global adoption of facial recognition technology with special reference to India—Present status and future recommendations”, *Medicine, Science and the Law*, Vol 64 Issue 3, January 2023. https://doi.org/10.1177/00258024241227717

[50] Degli Esposti, S. and Santiago Gómez, E., “Acceptable Surveillance-Orientated Security Technologies”, *Surveillance & Society* (13) 3-4, 437-454, 2015.

[51] Andrejevic M, Selwyn N, Gu X, Smith G, O’Malley P, O’Neill C (2024), op cit. p.12; Kugler op cit. p.25; and Ritchie, loc cit. p.21.

[52] Degli Esposti, S. and Santiago Gómez, E., Loc cit.

[53] Ritchie KL, Cartledge C, Growns B, Yan A, Wang Y, Guo K, et al. (2021) Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world, *PLoS ONE*, 16(10). https://doi.org/10.1371/journal.pone.0258241P.16.

[54] Kostka et al. (2021), Loc cit. p.679-6981.

[55] Adam Schwartz and Nathan Sheard, *Why EFF Doesn’t Support Bans On Private Use of Face Recognition*, 20 January 2021. https://www.eff.org/deeplinks/2021/01/why-eff-doesnt-support-bans-private-use-face-recognition

[56] Kat Krol, Simon Parkin, and M. Angela Sasse, “”I don’t like putting my face on the Internet!”: An acceptance study of face biometrics as a CAPTCHA replacement,” 2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), Sendai, Japan, 2016, pp. 1-7. https://doi.org/10.1109/ISBA.2016.7477235

[57] Matthew B. Kugler, “From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms”, UC Irvine Law Review, Vol 10, Issue 1, 2019. https://scholarship.law.uci.edu/ucilr/vol10/iss1/5

[58] Ibid.

[59] Kat Krol, et al., loc cit.

[60] Andrejevi, et al. Loc cit.

[61] Oliver Buckley, Jason R.C. Nurse, "The language of biometrics: Analysing public perceptions", *Journal of Information Security and Applications*, Vol 47, August 2019. P. 117. https://doi.org/10.1016/j.jisa.2019.05.001

[62] Matthew B. Kugler, "From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms", UC Irvine Law Review, Vol 10, Issue 1, 2019. https://scholarship.law.uci.edu/ucilr/vol10/iss1/5

[63] Sara H. Katsanis, et al., "U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics", *IEEE Transactions on Technology & Society*, Vol. 3, No. 1, March 2022.

[64] Lee Rainie, Cary Funk, Monica Anderson, Alec Tyson, "Public more likely to see facial recognition use by police as good, rather than bad for society", Pew Research Center, 17 March 2022. https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/

[65] Aaron Smith, "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly", Pew Research Center, 05 September 2019. https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

[66] Unisys Australia (2014). *Unisys security index report Australia: Biometrics in airports*, Sydney.

[67] Claire Galligan, et al., *Cameras in the Classroom: Facial Recognition Technology in Schools*, University of Michigan research report, 25 August 2020. https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schools

[68] Stop Facial Recognition on Campus. https://campus.banfacialrecognition.com/#sign

[69] Nahid Widaatalla, "AI and Facial Recognition Dive Into Global Health Care", Think Global Health, 06 May 2024. https://www.thinkglobalhealth.org/article/ai-and-facial-recognition-dive-global-health-care

[70] Sara H Katsanis, et al., "A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts", *PLOS ONE*, 14 October 2021. P.2. https://doi.org/10.1371/journal.pone.0257923

[71] Ibid. p.6.

[72] Kugler, op cit. p.12.

[73] *Beyond face value: public attitudes to facial recognition technology*, London, Ada Lovelace Institute, September 2019. P.9. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

[74] Final Report on Live Facial Recognition, London Policing Ethics Panel, Mayor of London, May 2019. P.23. http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

[75] Ritchie, loc cit. p.17.

[76] Kugler, op cit. p.2.

[77] Ibid. p.14.

[78] 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology

[79] Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). "Live facial recognition: Trust and legitimacy as

predictors of public support for police use of new technology", *The British Journal of Criminology*, 60(6),

1502–1522. https://doi.org/10.1093/bjc/azaa032. An examination of public perceptions of the use of FRT by police within body-worn cameras (BWC), for example, found that public support was reliant on the type and manner of surveillance such as whether it is used in real-time or after the fact, as well as the demographic surveyed within the sample. Bromberg, D. E., Charbonneau, E., & Smith, A. (2018). Body-worn cameras and policing: A list experiment of citizen overt and true support. *Public Administration Review*, *78*(6), 883–891. Bromberg, D. E., Charbonneau, E., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, *37*(1), 1–8. See also Adelaide Bragiasa, et al., loc cit. P.1650.

[80] Daniel E. Bromberg, Étienne Charbonneau, Andrew Smith, "Public support for facial recognition via police body-worn cameras: Findings from a list experiment", Government Information Quarterly, Vol 37, Issue 1, January 2020. https://doi.org/10.1016/j.giq.2019.101415

[81] *Beyond face value: public attitudes to facial recognition technology*, op cit.

[82] Nicholas Dynon, “UK Lords Committee questions legality of Live Facial Recognition Technology”, *New Zealand Security Magazine*, February-March 2024. https://defsec.net.nz/2024/03/10/uk-lords-committee-questions-live-facial-recognition-legality/

[83] Xiaojun Lai and Pei-Luen Patrick Rau, loc cit.

[84] https://www.rnz.co.nz/news/media-technology/525642/nz-police-finally-has-facial-recognition-policy-but-is-it-strict-enough

[85] James Sweetland, “The big FR debates: The operational value of facial recognition”, *Policing Insight*, 07 October 2024. https://policinginsight.com/feature/analysis/the-big-fr-debates-the-operational-value-of-facial-recognition/

[86] *Baltimore's Ban on Private Sector Use of Facial Recognition Technology Expires*, Hunton Andrews Kurth blog, 05 January 2023. https://www.huntonak.com/privacy-and-information-security-law/baltimores-ban-on-private-sector-use-of-facial-recognition-technology-expires

[87] *Beyond face value: public attitudes to facial recognition technology*, Ada Lovelace Institute, September 2019. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf *Beyond face value: public attitudes to facial recognition technology*, op cit.

[88] Carey Doberstein, et al., loc cit. p.208.

[89] Neil Selwyn, Gavin Smith, Mark Andrejevic, Xin Gu, Chris O'Neill, “Facing up to Problem Gambling: Tracing the Emergence of Facial Recognition Technology as a means of Enforcing Voluntary Self-Exclusion”, *Journal of Gambling Studies*, April 2024. https://doi.org/10.1007/s10899-024-10308-4

[90] *Facial recognition technology*, Consumer and Business Services, Government of South Australia. https://www.cbs.sa.gov.au/sections/LGL/facial-recognition-technology#:~:text=As%20part%20of%20the%20gambling,installed%20in%20their%20gaming%20rooms.

[91]

[92] Facial Recognition Technology (FRT), Alliance for Gambling Reform, Australia.

[93] https://fare.org.au/call-for-moratorium-on-facial-recognition-technology-use-in-alcohol-and-gambling-venues-across-australia/

[94] Matthew B. Kugler, “Public Perceptions Can Guide Regulation of Public Facial Recognition”, *Columbia Science and Technology Law Review*, Vol 25, No 1, Fall 2023. https://journals.library.columbia.edu/index.php/stlr/article/view/12380/6143

[95] Xiaojun Lai and Pei-Luen Patrick Rau, “Has facial recognition technology been misused? A public perception model of facial recognition scenarios”, *Computers in Human Behavior*, Vol 124, November 2021. https://doi.org/10.1016/j.chb.2021.106894

[96] Nessa Lynch, Liz Campbell, Joe Purshouse, Marcin Betkier, *Facial Recognition Technology in New Zealand*, New Zealand Law Foundation, November 2020. https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf

[97] Andrew Chen, *Facial Recognition Technology*, New Zealand Police, July 2024. New Zealand Council for Civil Liberties webinar, 16 August 2024. https://nzccl.org.nz/watch-the-police-and-facial-recognition-webinar/

[98] *Biometric Processing Privacy Code – Exposure draft only for comment*. Office of the Privacy Commissioner, New Zealand, April 2024.