Australian Attitudes to Facial Recognition: A National Survey

Whitepaper #01

Automated Society Working Group
School of Media, Film, and Journalism
Monash University

MONASH University

Automated Society Working Group

The Automated Society Working Group investigates the impacts of automation on Australians and the world.

Our research provides insights into advertising, surveillance, digital platforms, automated production, and entertainment.

We provide expert perspectives on the global shifts in information, data, regulation and telecommunications policy.

The Automated Society Working Group is based in the School of Media, Film, and Journalism in the Faculty of Arts, Monash University. Its members are:

Professor Mark Andrejevic, Lead

Dr. Robbie Fordyce

Dr. Luzhou Li

Dr. Verity Trott.

This report was produced with contributions from:

Professor Neil Selwyn (Monash Education)

Professor Liz Campbell (Monash Law)

Photograph credits:

p. 3, 7, 8, 18, 26 - Davide Ragusa

p.4 - Victor Rodriguez

p.6 - Victor Garcia

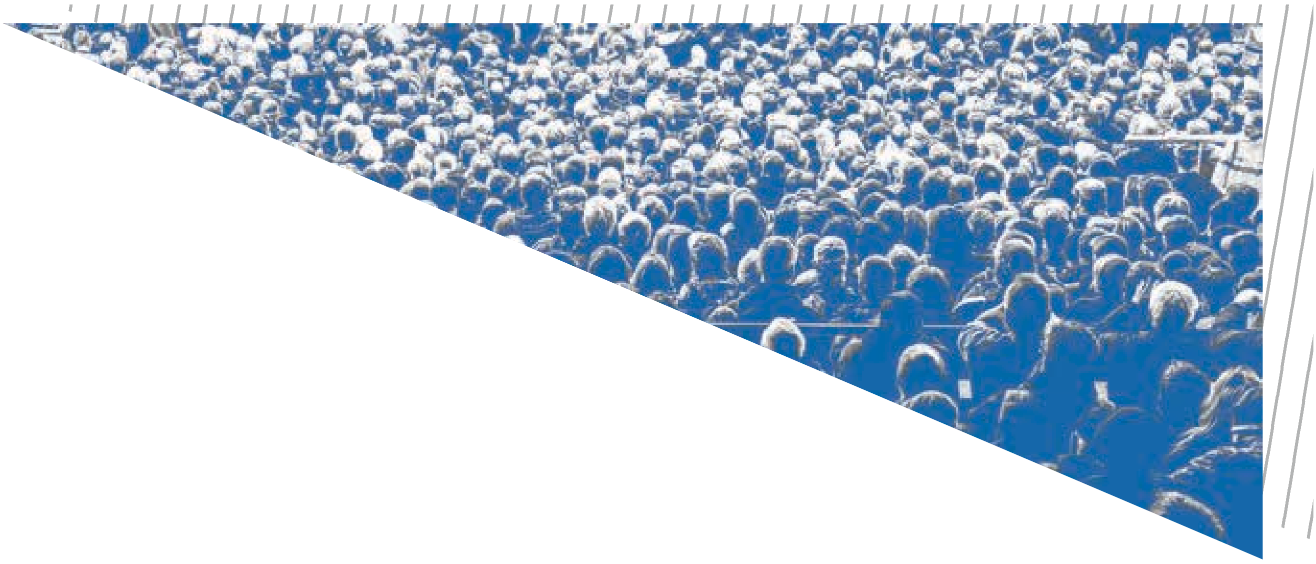
p.9 - Adrien Olichon

p.10 - NeONBRAND

p.17 - Jordon Conner

All photographs available freely at Unsplash.com

Published May 2020, Monash University



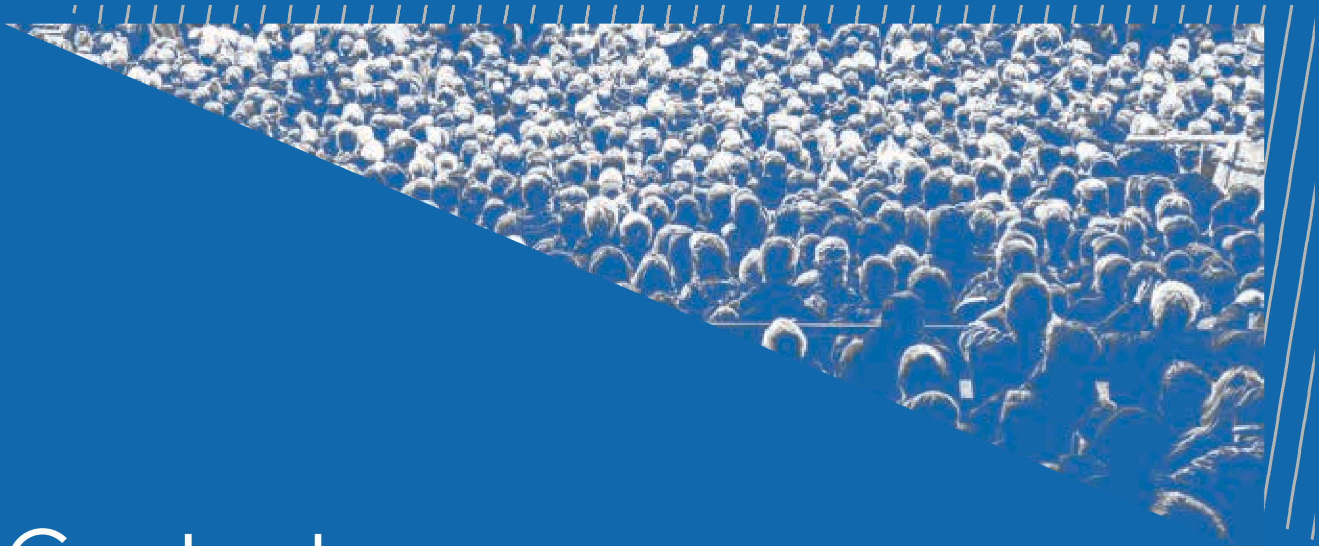
Executive Summary

Facial recognition technology is coming to play an increasingly important role in Australian society. The Federal Government is working toward the implementation of a national facial recognition database, and local municipalities, private schools, workplaces, and businesses are already starting to incorporate facial recognition technology into their security systems and marketing strategies.

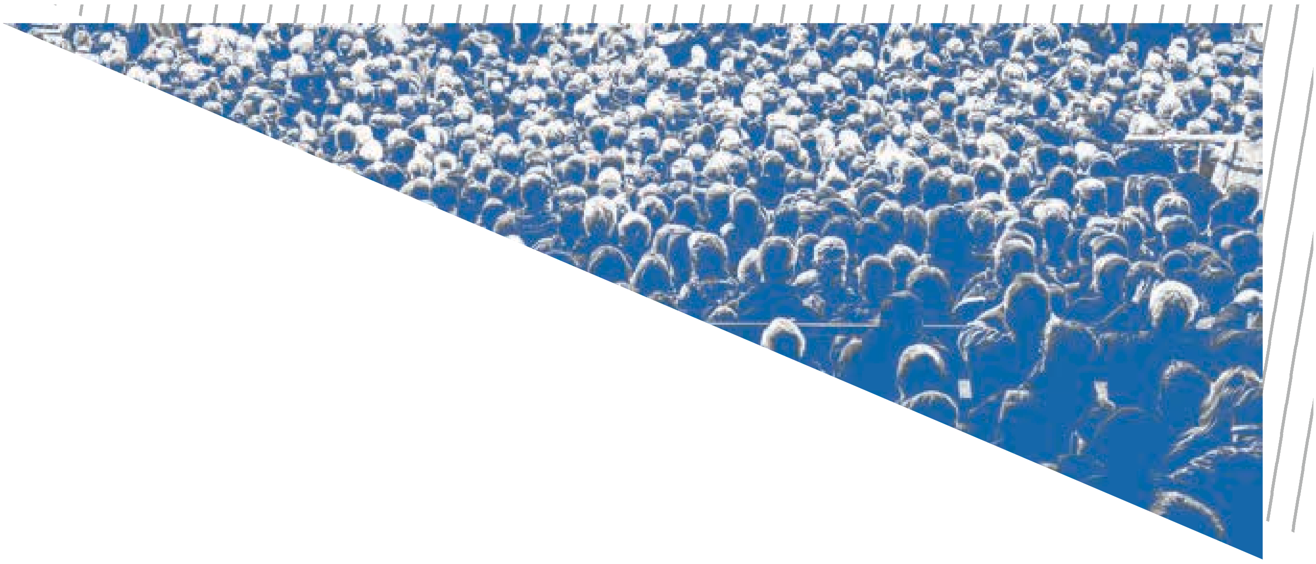
The technology is developing at a rapid pace, and one Australian citizen has received media coverage for developing a consumer-facing app that uses billions of images scraped from the Internet to identify people who appear in photos uploaded from a phone or any other source. This app, called Clearview AI, is already being used by Australian Federal Police as well as State Police in Queensland, Victoria, and South Australia. Proposed commercial and public uses for facial recognition technology include targeted marketing, shopping, ATM access, mass transit, employee and student tracking, and much more. Many of these applications are being developed and rolled out without robust public discussion and debate -- and with minimal regulatory attention or public engagement.

The findings of this survey reflect a tension between concerns about privacy and support for a technology that offers the promise of more effective security and law enforcement. Almost half of those surveyed (49%) felt that the use of facial recognition technology in public spaces constituted an invasion of privacy, and more than a third of the respondents -- a plurality -- agreed that, “The risks of using facial recognition technology outweigh the benefits,” whereas more than 60% felt that they should have the right to opt out of any facial recognition database -- an option that would greatly reduce the utility of a facial recognition system. More than a third (36%) described it as too inaccurate to be practical, and a similar number (37%) said the risks of using the technology outweigh the benefits.

Nonetheless, 61% of respondents said it could be a useful tool for public safety. This pattern repeated itself for many of the uses of the technology covered by the survey. In general there was support for the use of the technology for security and policing purposes. Respondents were concerned about the accuracy of the technology (36%) and the possibility that it may be biased (37%). Almost two-thirds of respondents expressed concern about the security of facial recognition databases, whereas 50% said they would have no concerns about the use of the technology as long as they were made aware of when and where their data was being used and stored.



Contents



Methodology

In order to assess public attitudes toward the development of facial recognition technology for a range of purposes, The Automated Society Working Group at Monash University commissioned a nationwide survey, the results of which are summarized in the following pages. The survey was conducted by Melbourne-based WhereTo Research Consultants using the company's nation-wide panel. It summarizes the responses of 2,291 people and has been weighted by SES, CALD (cultural and linguistic diversity) and education to represent the Australian population.

Participants were screened and provided basic demographic data. All participants were over the age of 18 at the time the survey was conducted. Our initial questions determined the degree of knowledge and use of facial recognition technology:

> 9 in 10 (88%) Australians have heard of facial recognition technology, less than 1 in 10 (8%) feel they know a lot about it.
>
> 34% have used facial recognition/scanning as a form of identity verification (61% have only heard of it)

Participants were asked questions across three topic areas: awareness of facial recognition, views on technology, attitudes and perceptions. Participants were provided with both multi-choice and short-answer questions.

From our data we made these general observations about the responses:

3 in 5 feel their personal data is not safe and secure (10% extremely safe and secure).

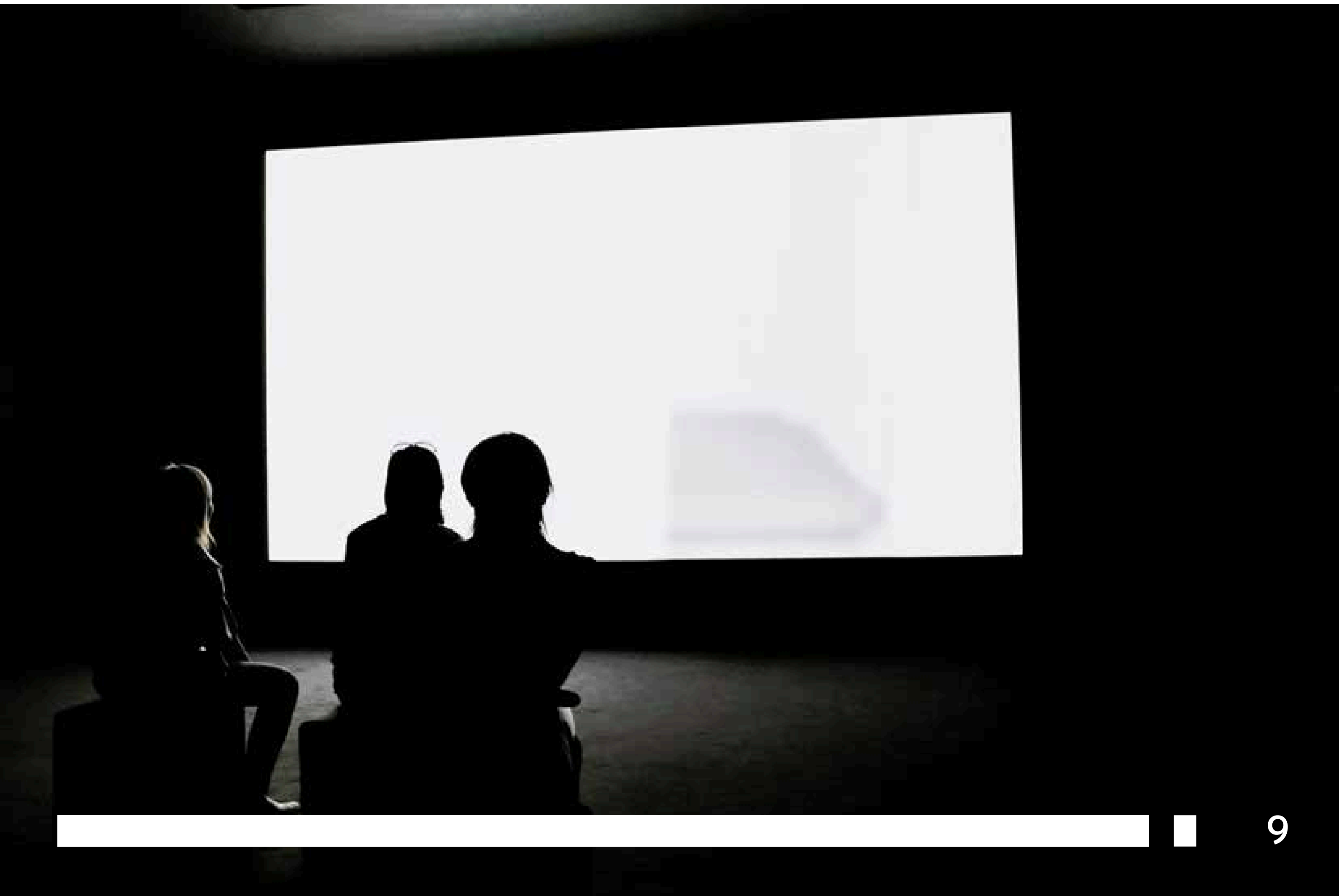
61% of Australians feel that facial recognition technology could be an important tool for improving public safety, however 64% feel that databases are not safe enough from hacking or cybertheft.

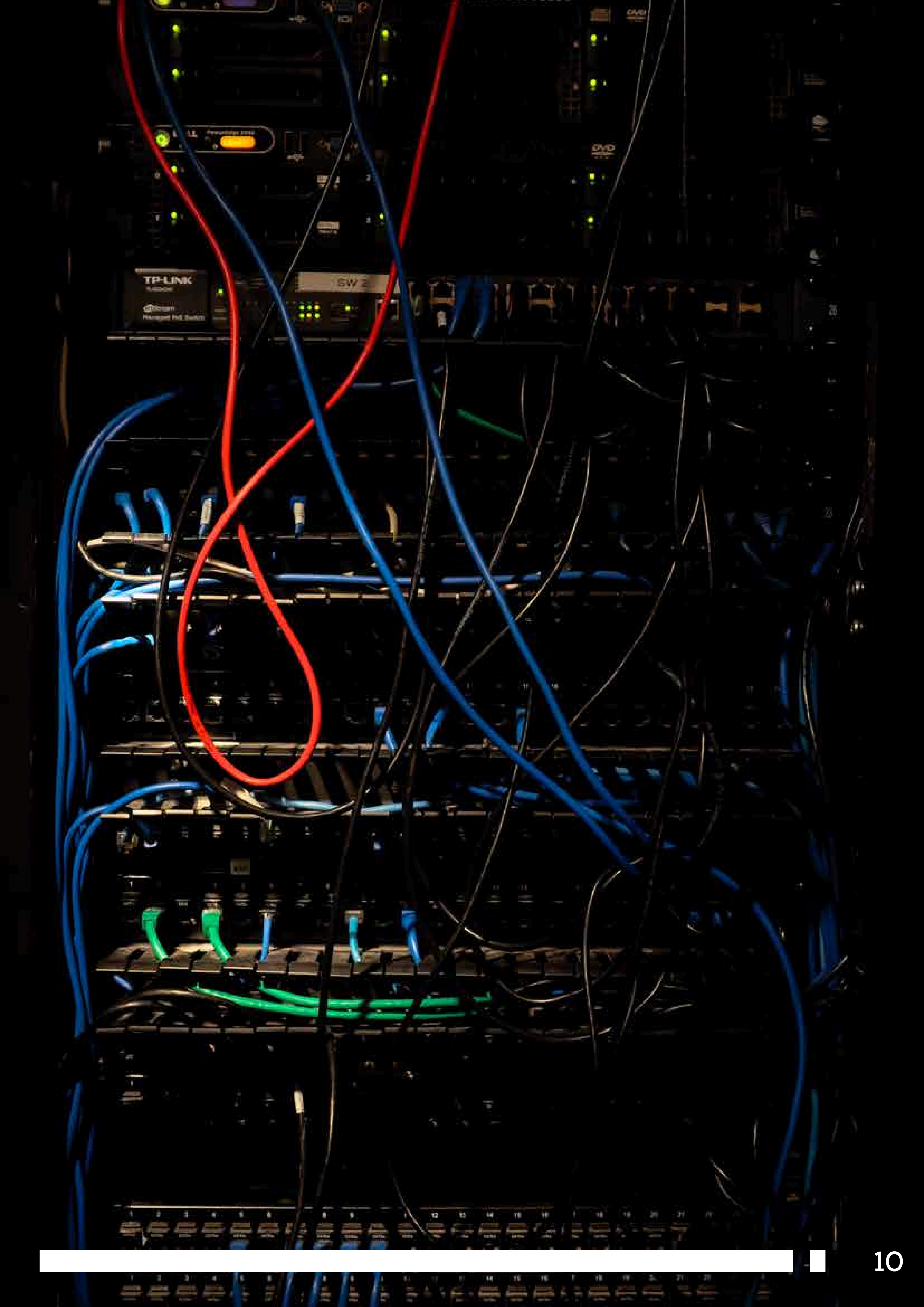
15% strongly feel that protecting our national security is more important than protecting the privacy of individuals.

Participants are generally unaware of implicit consent but use a discourse of 'rights to personal data' to describe normative expectations.

Participants were agnostic with regards to which types of technology could be used to identify them; i.e. for those that expressed concern, there was little distinction between CCTV, fingerprinting, iris scanning or other identification technologies.

Participants trusted schools, the police, and workplaces a great deal, while participants overwhelmingly distrusted foreign governments.

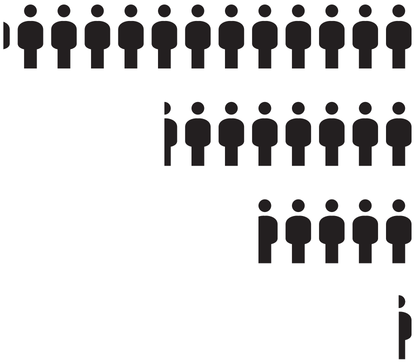



TP-LINK
SW 2
DVD

Privacy Concerns

Question

“Use of facial recognition technology to **identify** people in **public places** is an **invasion of privacy**.”



49% Agree or Strongly Agree

30% Neither Agree nor Disagree

19% Disagree or Strongly Disagree

02% Don’t Know/Can’t Say

A nationwide representative survey of Australians’ attitudes toward the use of facial recognition technology has found that almost half of respondents think its use in public places is, “an invasion of privacy.” 49 percent of respondents either agreed or strongly agreed with the statement that the “Use of facial recognition technology to identify people in public places is an invasion of privacy.” Only 19% of respondents disagreed or strongly disagreed with this statement. Almost a third neither agreed or disagreed.

“What first comes to mind when you think of facial recognition technology?”

“...law enforcement.”

“...criminals getting caught, privacy being eroded.”

“...abuse by the Police and other authorities.”

“...tracking, invasion of privacy.”

“...Orwell's 1984.”

“...invasion of privacy.”

“...does it have to be updated as your face ages?”

“...those dystopian future movies where the government tracks your every move.”

“...not sure of accuracy, don't know if I would wholly trust it.”

“...I use it on my iPad and I think it is a good way to protect youself.”

“...a tool to be used by law enforcement agencies to identify people of interest.”

“...maybe it is used by police and detectives to try to identify someone who has committed a crime.”

“...Used in security services to identify suspects. High levels of data resourcing and analytics.”

“...Privacy issues. I don't like the idea that everything I do is being watched by someone.”

“...Big Brother - I hate this technology - it is invasive and a loss of privacy. If police use it it could easily cause innocent people to be convicted based on a computer's findings. Its bad enough having cameras spying on you in the street without this added level of scrutiny.”

“...would be beneficial for places like airports to speed up boarding processes as well as make sure people are who they say that are, however it can also be a very risky technology if it falls into the wrong hands or is used maliciously.”

“...I don’t feel comfortable with facial recognition. I’m sure it’s incredibly useful. I prefer relative anonymity and wouldn’t want my facial patterns stored, same as my fingerprints, unless I was legally obligated to give them.”

“...I think of criminals being recognised in crowds by cameras scanning everyone's faces. I also think of airport security and future general security measures.”

“...technology capable of identifying or verifying a person from a digital or video frame from a video source.”

“...Facial recognition technology has been utilised in our latest smart phones, it scans and recognises the face of the owner of the mobile phones to unlock the phones, facial recognition is also utilised in highly sensitive work areas to unlock and provided access for individuals to access certain highly secured areas..”

“...big brother. This technology can tell whoever is using it where you are/were time etc.”

First Responses

Our respondents were given the chance to provide their thoughts on what came to mind when they first thought about facial recognition. Positions varied, partly based on personal experience.

Some people reflected on the way that it helped them to use existing technology such as their own phones, or thought about the way that it replaced things like fingerprints and other biometric indicators.

Other responses focused on a significant concern around privacy; concern that the technology is inaccurate; that it is tied in with illegal or corrupt government behaviour; that it cannot be trusted; and that it is only ever used punitively.

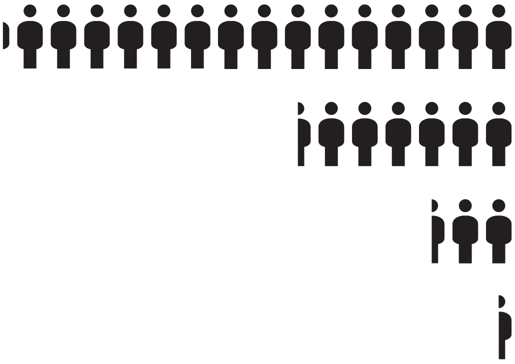
Many respondents noted that even in cases where respondents describe facial recognition as having positive public safety outcomes, the technology was considered to be ‘creepy’, with overtones of excessive government intervention in daily life.

In an overwhelming number of responses, facial recognition technology has been understood as a security technology, whether for managing personal devices or as a part of state surveillance mechanisms.

Public Safety

Question

“Facial recognition technology **could be** an important tool for **improving public safety**”



61% Agree or Strongly Agree

26% Neither Agree nor Disagree

10% Disagree or Strongly Disagree

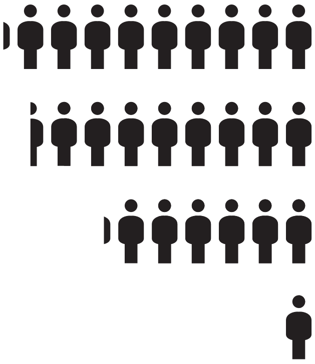
02% Don’t Know/Can’t Say

However, the overall assessment of the technology reflected competing tendencies. Despite concerns over privacy and the risks of the technology, a majority of respondents (61 percent) either agreed or strongly agreed with the claim that “facial recognition technology could be an important tool for improving public safety”).

Risks vs. Benefits

Question

“The **risks** of using facial recognition technology **outweigh the benefits**.”



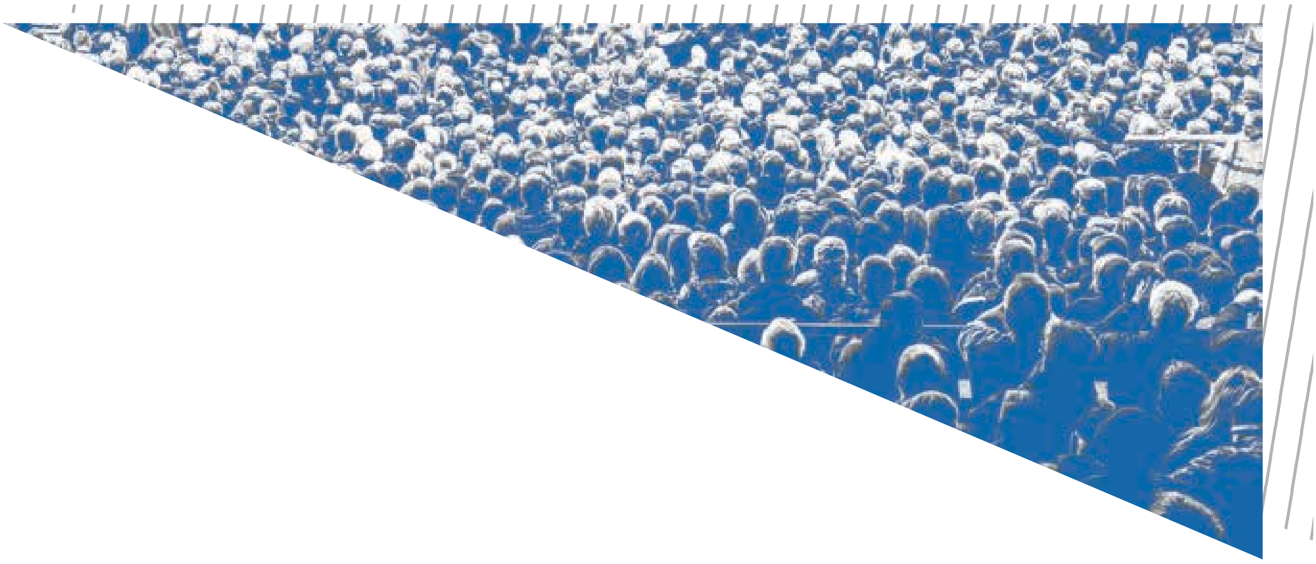
37% Agree or Strongly Agree

34% Neither Agree nor Disagree

25% Disagree or Strongly Disagree

04% Don’t Know/Can’t Say

More than a third of the respondents -- a plurality -- agreed or strongly agreed with the claim that, “The risks of using facial recognition technology outweigh the benefits.” However, an almost equally large number neither agreed nor disagreed.



Trust

One of the primary concerns that is most visible in the public domain is the degree of trust that people have in the institutions that make and deploy facial recognition. Trust covers a range of vague expectations that represent the way that people expect data to be used. People who trust institutions do so because they expect their own data not to be misused, and that their data is kept private and secure. People trust the federal government to use facial recognition in security and border control contexts, but are less trusting of facial recognition in state or local contexts. We read this as a generalised expectation that technology be used ‘out there’ on ‘other people’, while the use of the technology in familiar or local places represents more of an intervention in their daily lives.

Over the next pages we present findings from our survey where we asked respondents whether they trusted or distrusted different institutions and organisations. Depending on their response to our questions about the Federal Government, Private Sector Companies, and Schools, we asked them to rank their reasons for trusting or distrusting those organisations.

Comparing Trust

Most trusted organisations

The Police	61%
Schools	49%
Australian Federal Government	45%
Workplaces	43%
State Government	42%
Local Council	36%
Private Sector Companies	29%
Foreign Governments	18%

Most distrusted organisations

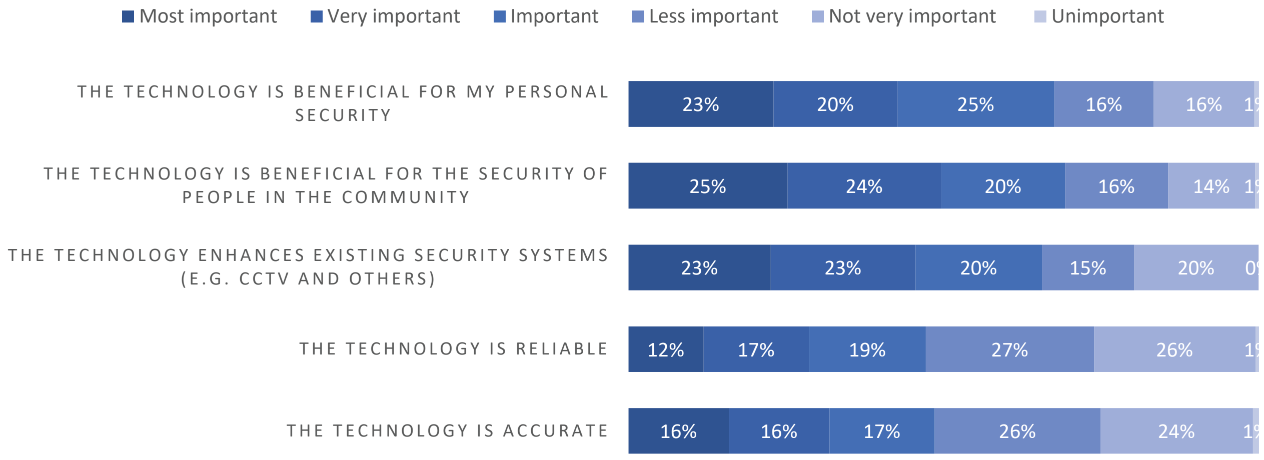
Foreign Governments	50%
Private Sector Companies	33%
Australian Federal Government	26%
State Government	27%
Local Council	27%
Workplaces	18%
Schools	16%
The Police	15%

Studying facial recognition also means studying the institutions that are seen to use, or maybe use, the technology. Facial recognition is often connected with ideas of Big Brother, or faceless governments retaining control over large volumes of data with minute details on the lives of everyday people. This is where a great deal of responses seem to locate their concerns about the technology. It's not the technology itself, per se, it's who owns the data and how it is used beyond the stated intent.

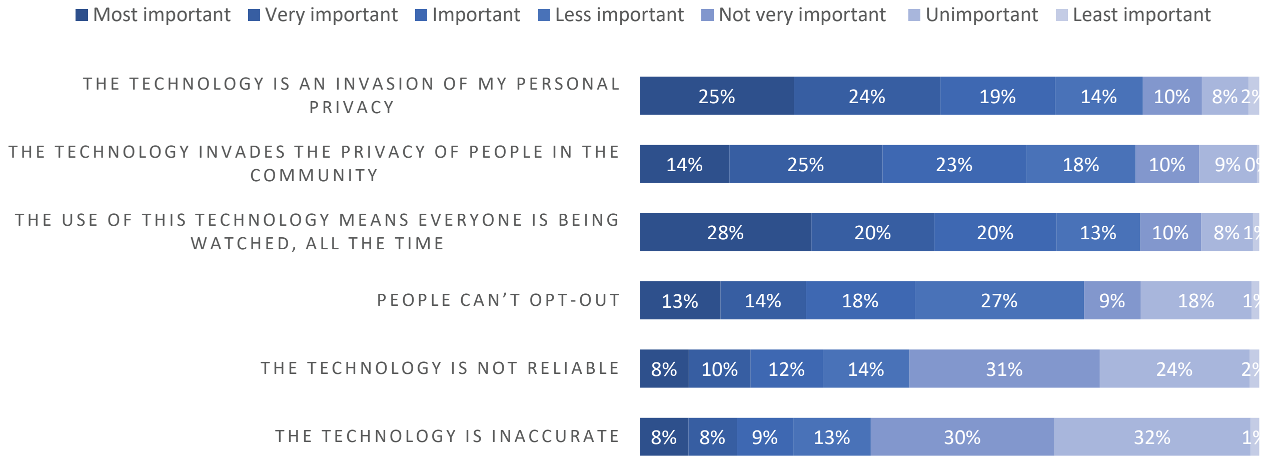
For this portion of the study we asked respondents to note whether they trusted or distrusted different categories of institution, ranking up to three each for 'trusted' or 'distrusted'. Generally speaking, we can see a tendency for public services like policing and schools being potentially trusted with facial recognition data. At the same time, private sector companies and foreign governments - which often produce technology or govern housed data - were significantly distrusted relative to institutions based in Australia.

Trust in Federal Govt.

“What are the main reasons for your **trust** in the development and use of facial recognition technology **in the federal government**?”

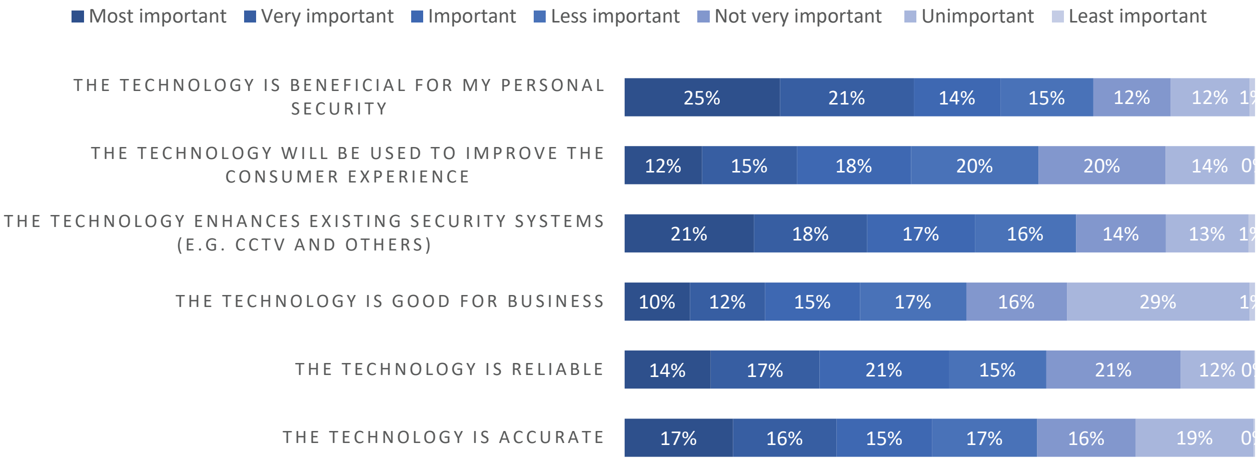


“What are the main reasons for your **distrust** in the development and use of facial recognition technology **in the federal government**?”

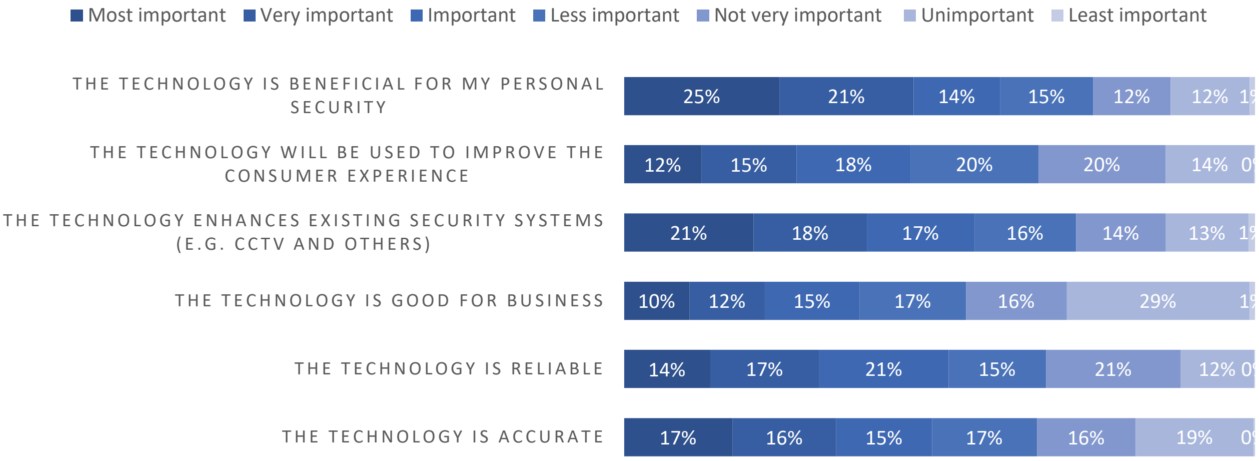


Trust in Private Sector

“What are the main reasons for your **trust** in the development and use of facial recognition technology **by private sector companies**?”

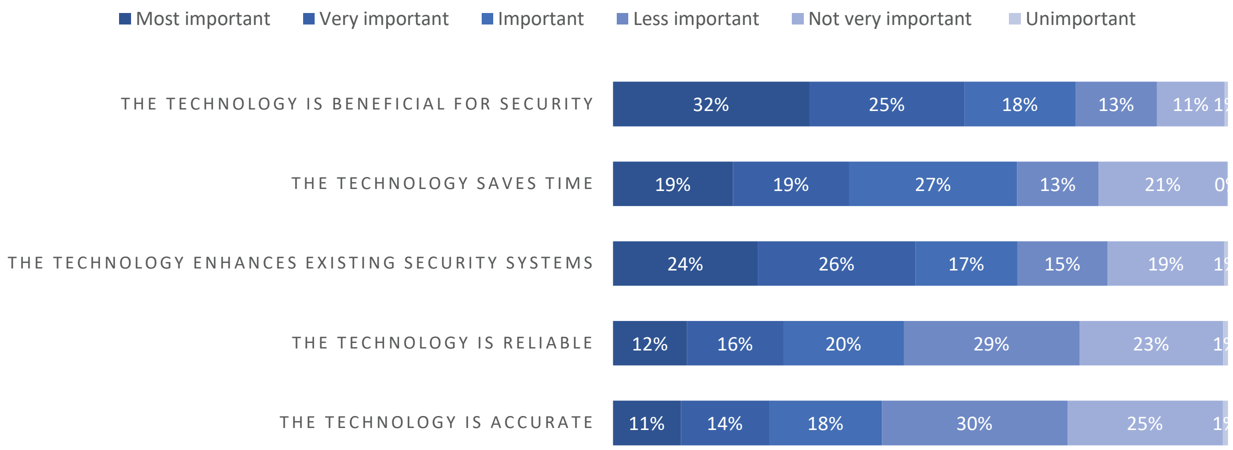


“What are the main reasons for your **distrust** in the development and use of facial recognition technology **by private sector companies**?”

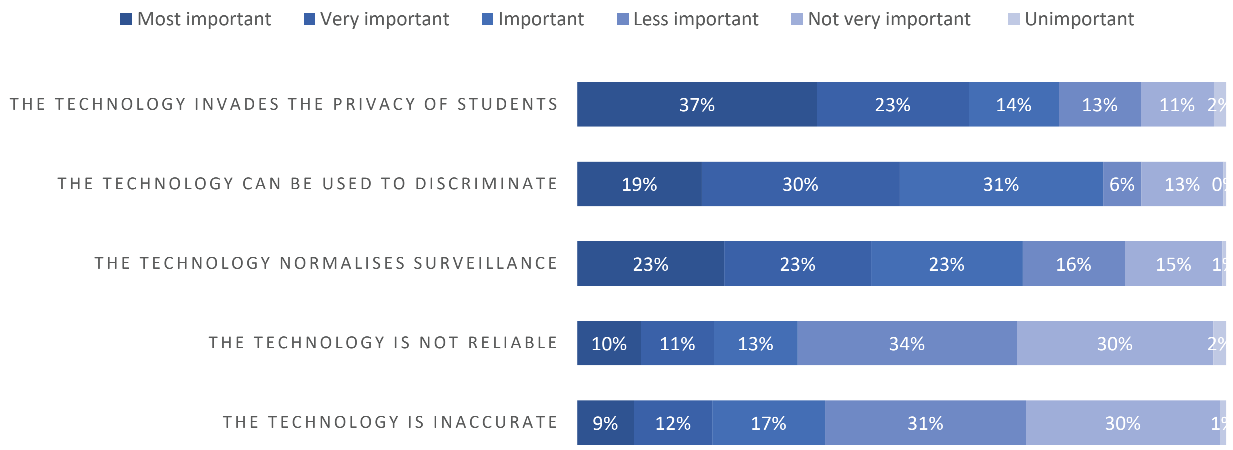


Trust in Schools

“What are the main reasons for your **trust** in the development and use of facial recognition technology **in schools**?”



“What are the main reasons for your **distrust** in the development and use of facial recognition technology **in schools**?”



Trust/ Distrust

Opting-Out of the Database

In keeping with privacy concerns, the majority of respondents said that Australians should be able to opt out of facial recognition databases -- a provision that, if enacted, would render it difficult to use the technology for many of its proposed security functions.

Accuracy

The responses also revealed a concern about the accuracy of the technology, with more than a third of respondents (36%) agreeing or strongly agreeing with the statement that "Facial recognition technology is not accurate enough to be practical." However, an almost equal number of respondents neither agreed nor disagreed with this claims. Less than a quarter disagreed.

Bias

Recent research has revealed that many facial recognition systems work better on some skin tones than others, and that accuracy can also vary by sex. Concerns about bias in the technology were reflected in the survey responses, with the largest group or respondents (37%) agreeing or strongly agreeing with the statement, "I am concerned about racial bias in facial recognition technology."

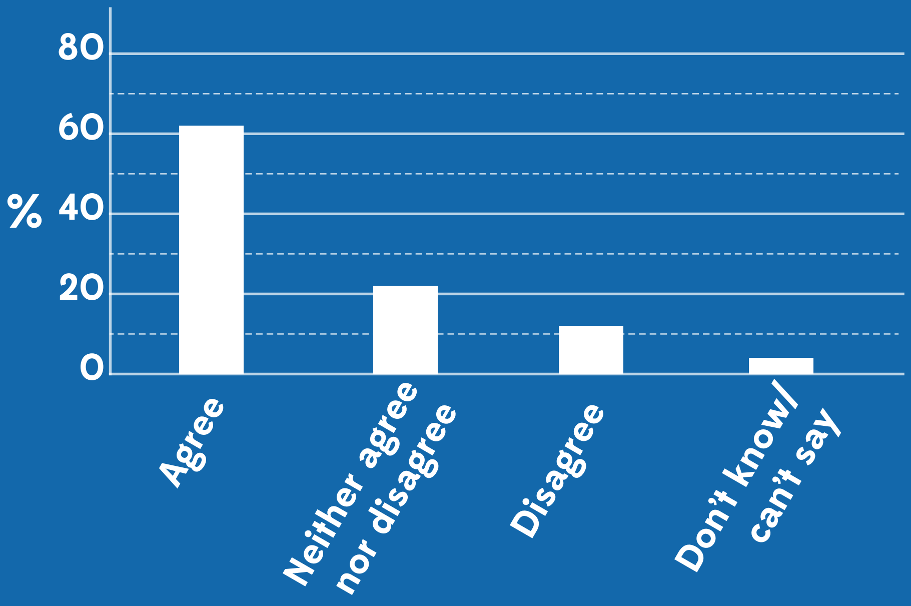
Security

Survey responses revealed a high level of concern (64%) about the security of the databases upon which facial recognition systems would necessarily rely, with a clear majority of respondents agreeing or strongly agreeing with the claim that, "Databases aren't safe enough from hacking or cybertheft."

Transparency

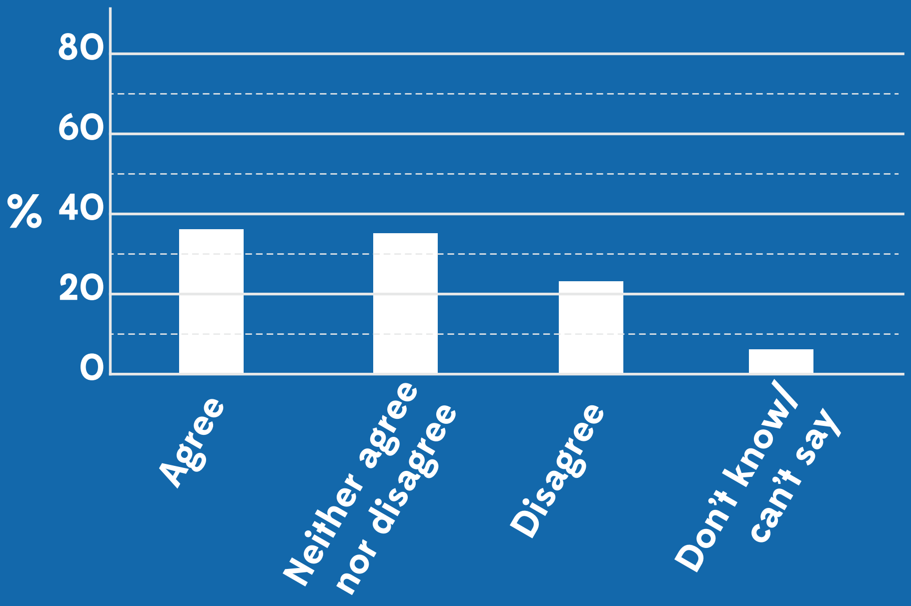
Despite issues of bias, security, and accuracy, a half (50%) of respondents agreed that they would have no concerns about the use of the technology as long as they were made aware of when and where their data was being used and stored.

Trust Factors



Question

"People should be able to **opt out** of having their photos added to **any facial identification database**"

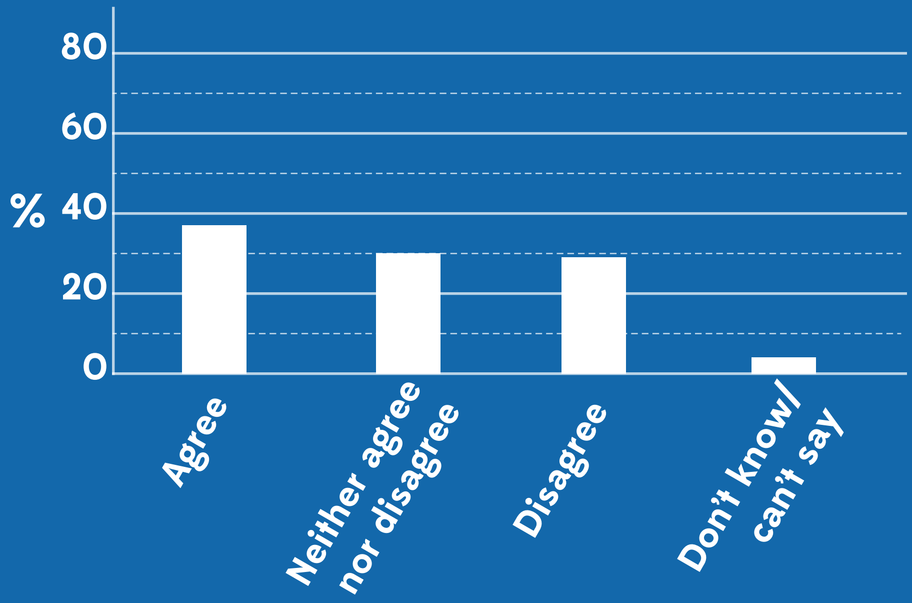


Question

"Facial recognition technology is **not accurate enough** to be practical"

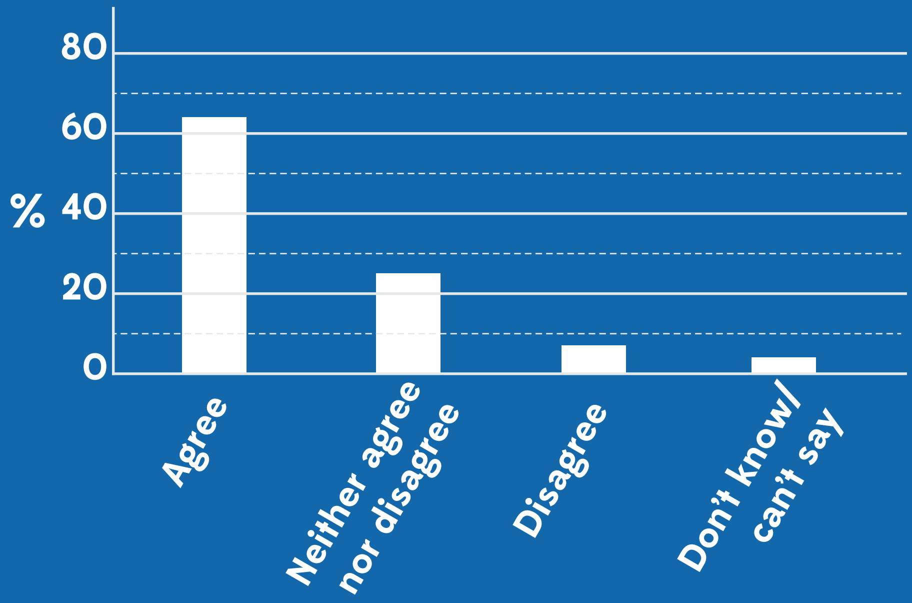
Question

“I am **concerned** about **racial bias** in facial recognition technology”



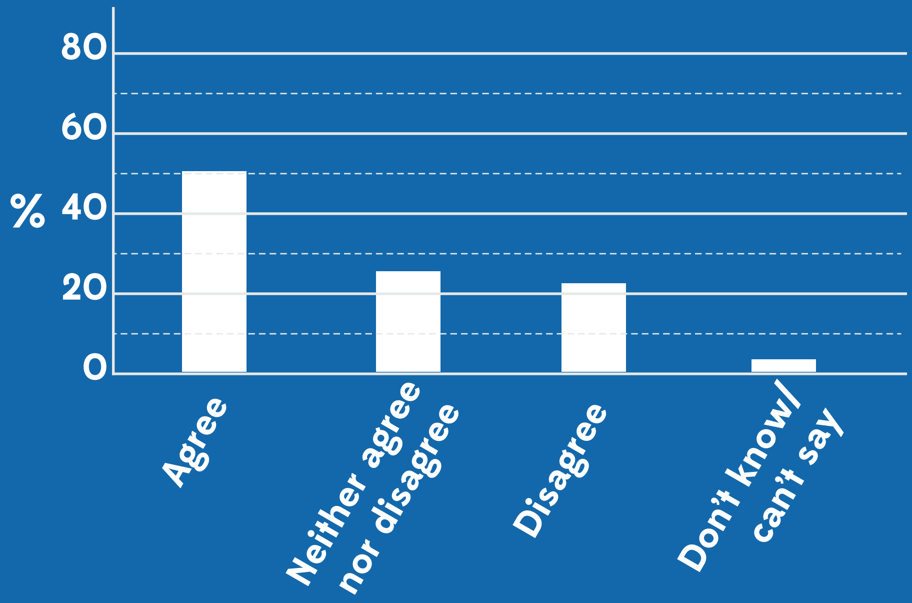
Question

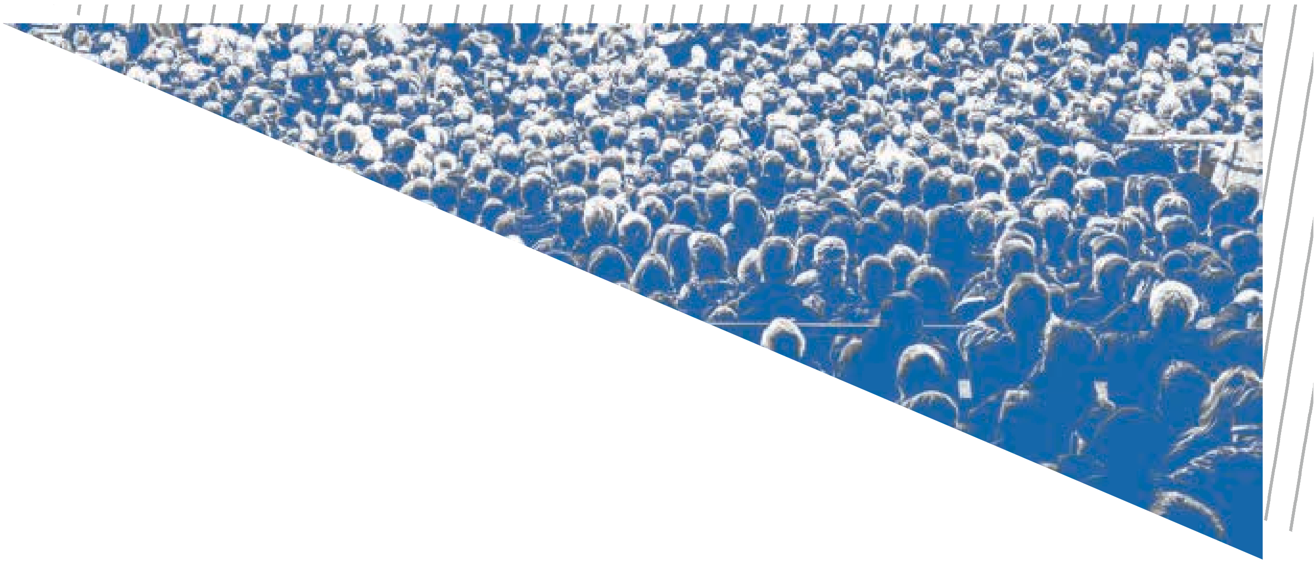
“Databases **aren’t safe enough** from **hacking** or **cybertheft** to guarantee facial recognition databases **won’t fall into the wrong hands.**”



Question

“As long as I am **made aware** of when and where my data is being **used and stored**, I have no concern with facial recognition technology capturing my data.”





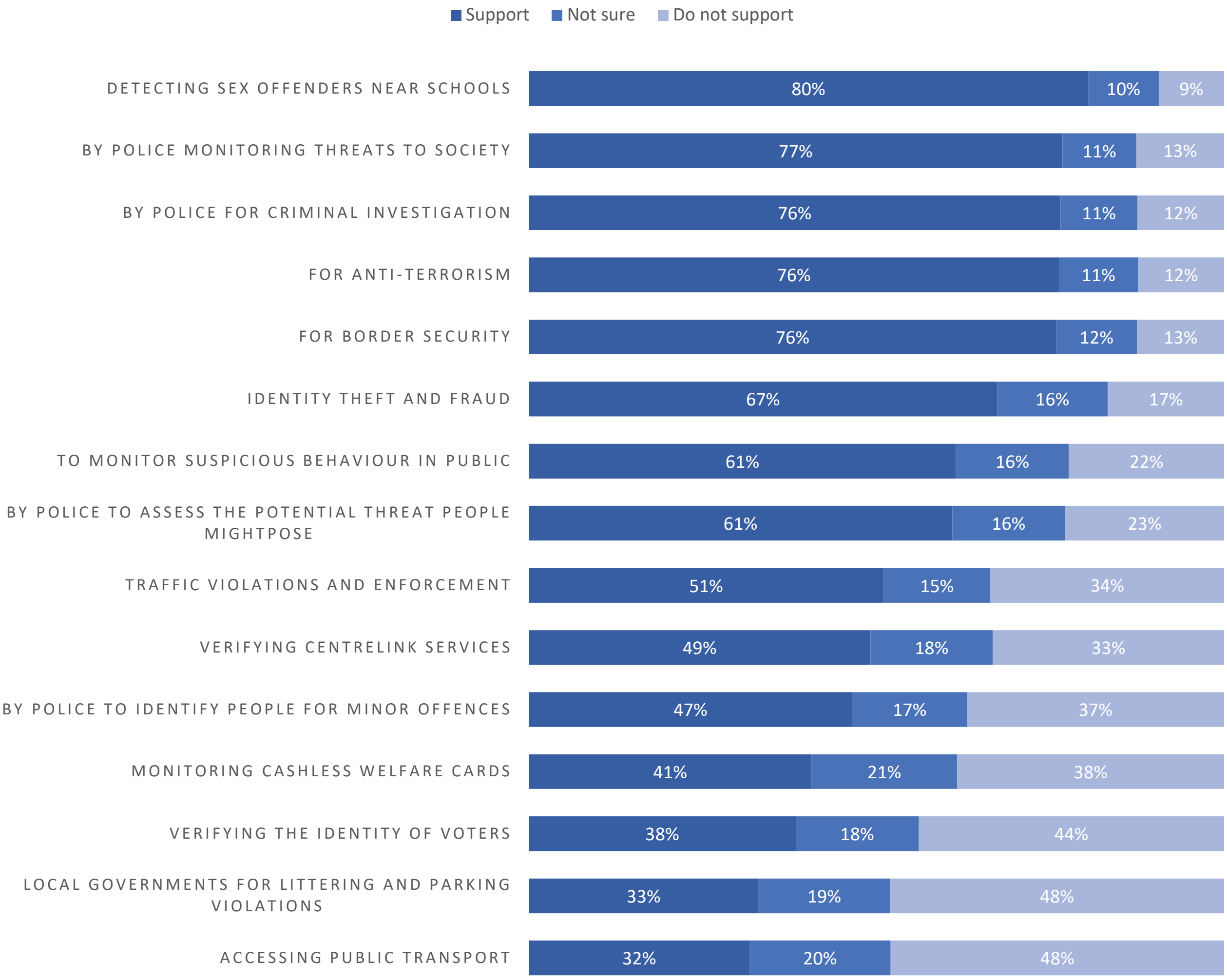
Support for Use Cases

Despite the varied concerns regarding providing data to different institutions, respondents did vary in terms of the specific use cases where they saw facial recognition as being useful. We note that there is higher support for cases where significant trauma or health impacts is a primary risk. There was significantly less support for the use of facial recognition for situations where surveillance would be employed for the purpose of automating fines or infringement notices for low-risk anti-social behaviours. For cases where there is a purely social utility (i.e. identifying individuals for government services such as voting or welfare) there was little direct support.

In cases of commercial use, facial recognition was deemed more acceptable if it was used for managing potentially illegal behaviour or for security purposes in public places; use of facial recognition as a 'convenience' device for advertising or access control was generally seen as undesirable, with the majority of people not supporting these use cases. Workplace uses of facial recognition were generally the least-supported use cases overall, likely due to the implication that the respondents would potentially be subject to these measures on a daily basis, unlike border security measures. Use cases were more supported the more that they facilitated work, and less as they involved surveillance of workers. Use of facial recognition in schools was seen as less desirable when it was accompanied by a specific use case; this is despite the relatively high trust in schools themselves.

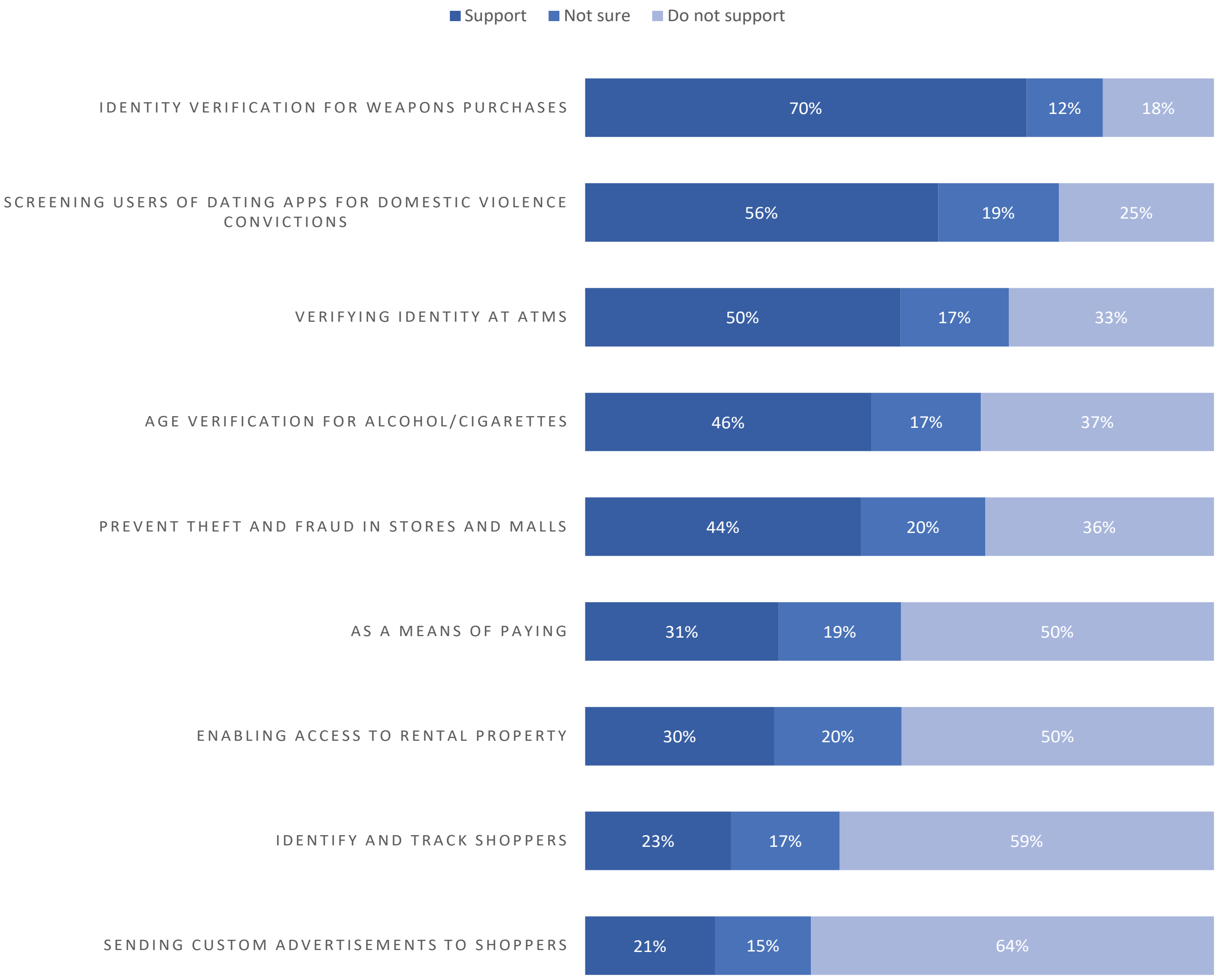
Ranking: Social Use Cases

“Please indicate whether you support the government use of facial recognition technology **using a national database** for the following purposes:”



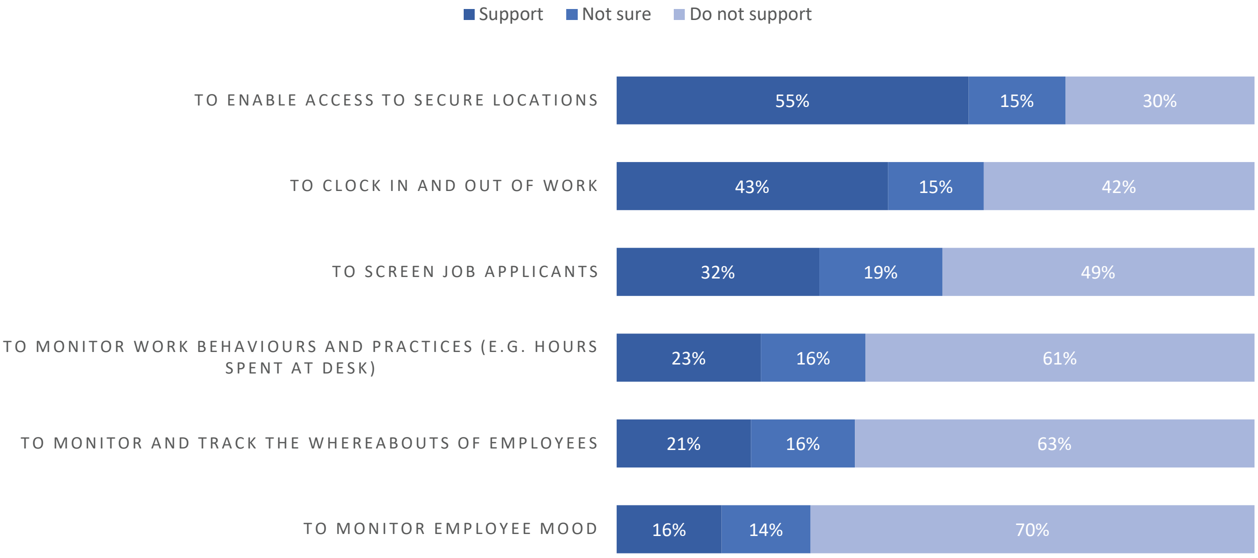
Ranking Commercial Use Cases

"Please indicate whether you support the use of facial recognition technology **by commercial organisations**:"



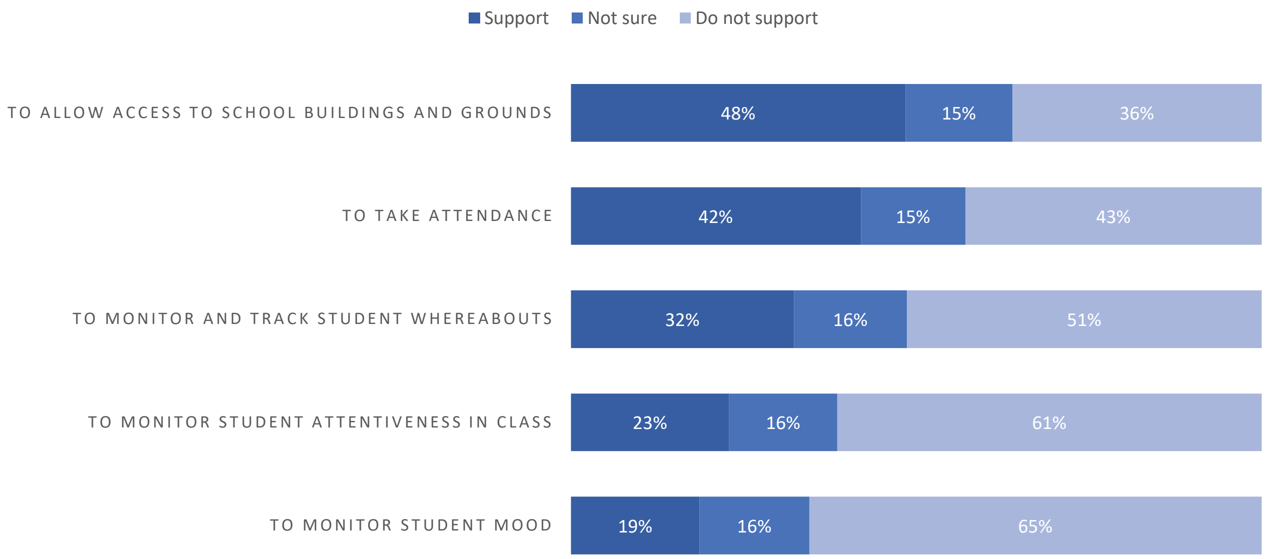
Ranking Workplace Use Cases

“Please indicate whether you support the use of facial recognition technology **in the workplace** for the following purposes:”

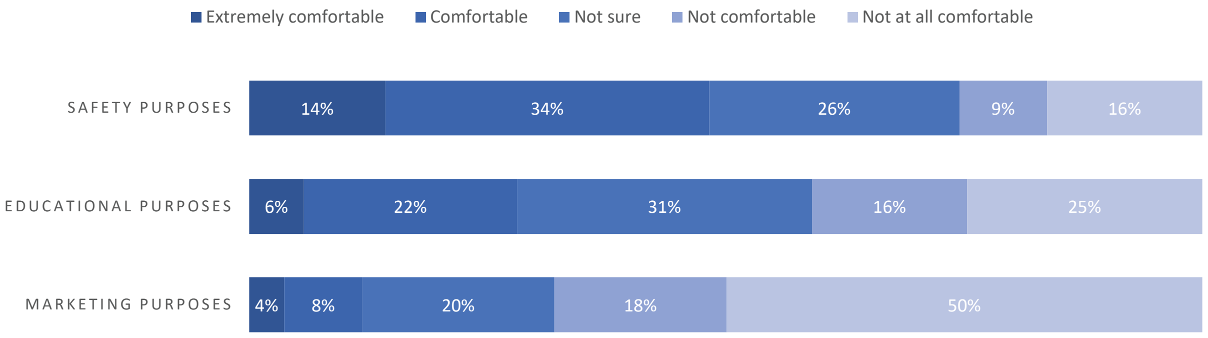


Ranking
School Use Cases

"Please indicate whether you support the use of facial recognition technology in schools for the **following purposes**:"



"How comfortable are you with facial recognition technology being **used to identify children under the age of 18** in the following contexts?"



Conclusions

Facial recognition is a technology that is only moderately-well understood by Australian civilians. The greater emphasis on support from our respondents referred to use cases that were unlikely to disrupt their own lives a great deal, and generally focused on being used in cases which led to the surveillance and databasing of others' lives.

There were concerns about the degree to which ownership and control of facial recognition data was a possible security risk, the greater interest was in controlling sites that were seen as involving specific risks to security where loss of life or significant trauma could be involved.

Respondents were broadly supportive of the use of facial recognition even in cases where it was seen as inaccurate or biased around matters of race, which suggests that users potentially see facial recognition as a part of heightened deterrance methods. This should be contextualised against the survey themes of border security and schooling. Even though respondents noted concern, they accepted facial recognition in contexts where racialised bias is more significant.

A significant and vocal group expressed opposition to all implementations of facial recognition, and rejected its use in most cases. This included lengthy qualitative responses and well-established claims of risks to various social liberties, and concern about increased government intervention in daily life.

An academic research paper is currently being drafted that addresses these findings in greater detail.

Contact the Automated Society Working Group to be notified of its release:

automated.society@monash.edu