

Australian Public’s Support of Facial Recognition Technology Depends on What Circumstance it is Used

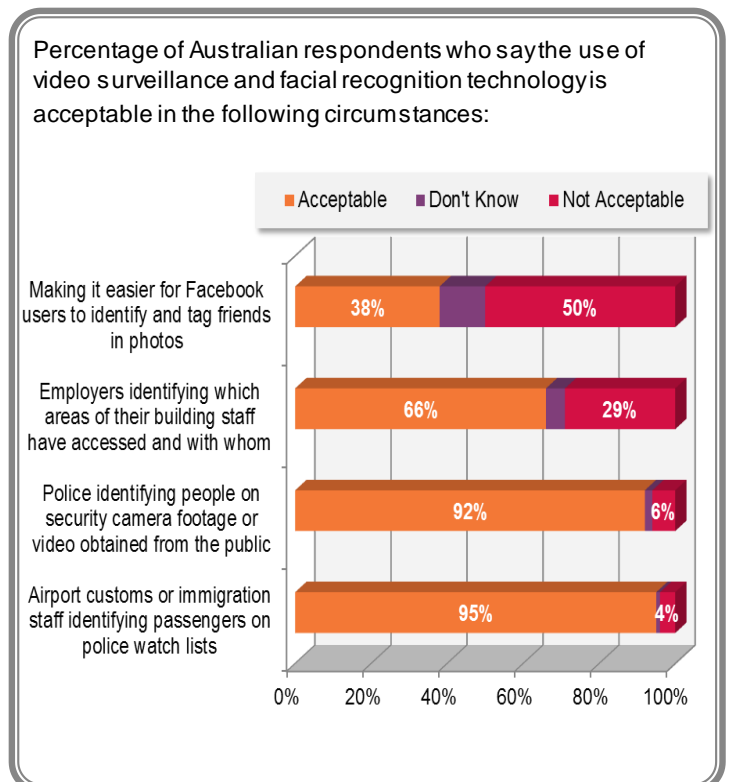
Australia on Facial Recognition

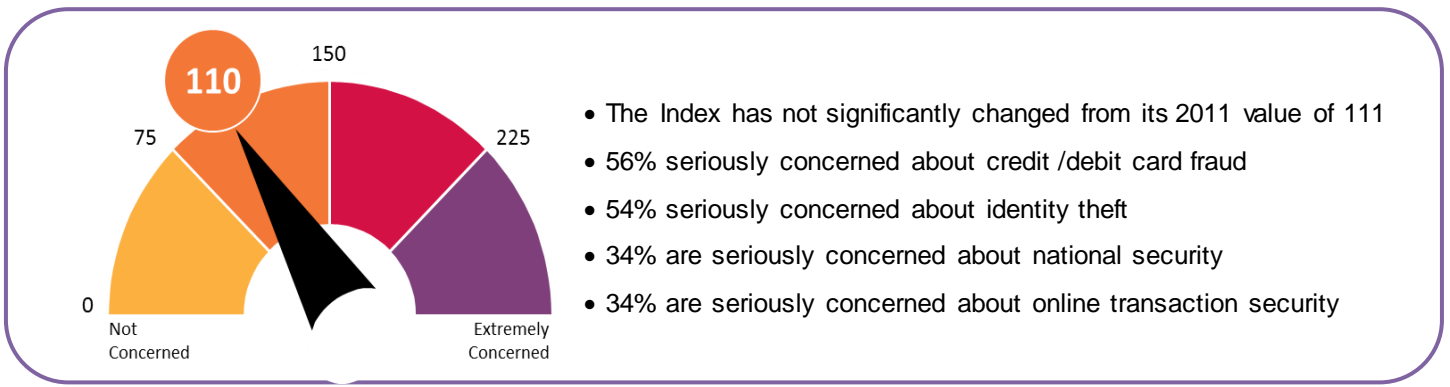
As part of the Unisys Security Index™, we regularly survey Australians on a range of security issues.

Facial recognition software can be used to identify people in videos or photos. This time we asked the Australian public if they found it acceptable to use facial recognition technology in four different scenarios. The research found that:

- 95 percent of Australians surveyed supported airport customs or immigration staff using facial recognition to identify passengers on police watch-lists.
- 92 percent of respondents agreed with the use of facial recognition technology to help police identify people from security camera footage or video obtained from the public.
- While 66 percent said it was acceptable for employers to use facial recognition to identify what parts of a building staff had accessed and with whom, 29 percent opposed the idea.
- Only 38 percent said it was acceptable for Facebook to use facial recognition technology to make it easier for users to identify friends in photographs while 50 percent said it was not acceptable.

The research findings clearly show that the Australian public varies its support of facial recognition technology depending on when, where and why it is being used. Support is strong in those circumstances that the Aussies deem to be appropriate such as policing or protecting borders. However the level of support falls significantly for a social media site using facial recognition technology. The moderate level of support for employers using facial recognition technology suggests that many Aussies find it acceptable for employers to monitor who accesses what part of a building.





Unisys Security Index – Australia

The overall Unisys Security Index for Australia has remained steady at 110 out of a possible 300 – its lowest level in the history of the survey.

The study shows that data privacy issues are still the top security concern for Australians with

- 56 percent of Australians extremely or very concerned about other people obtaining or using their credit/debit card details, and
- 54 percent extremely or very concerned about unauthorised access to or misuse of their personal information.

Unisys Perspective on Security

Organisations are waking up to a hostile IT infrastructure riddled with vulnerable mobile devices, poorly authenticated users, and multiple data and application security vulnerabilities that cyber criminals are exploiting with increasing frequency, sophistication and scale. Protection in such an environment is no longer just about securing the IT network perimeter.

Unisys believes that organisations can reduce risk and cost of security by analysing threats in both the cyber and physical worlds; creating tiered levels of user identity/access; monitoring an integrated environment; and taking advantage of devices with built-in advanced authentication to proactively protect against attacks on sensitive data, applications and mission-critical infrastructure assets.

What Organisations Must Do

- Establish a holistic cybersecurity framework to protect enterprise data and networks from internal and external threats.
- Manage user identities and entitlements through an integrated approach to lower audit reporting costs by centrally managing digital user identities and reduce critical employee errors with continuous messaging and policy implementation.
- Leverage built-in capabilities of next generation devices that allow advanced authentication via biometric techniques like voice, signature and facial recognition rather than deploying additional hardware.
- Adopt a coordinated approach to Sensitive Data Protection to recognise the reality of data volume that needs protection and establish automated ways to analyse and monitor large volumes of data.

How Unisys Can Help

Unisys Security Advisory Services

Analyses an organisation's current state against prevailing industry guidelines, and standards-based security practices. The assessment provides parameters for developing policies and systems to prevent internal and external data breaches.

Unisys Stealth Security

Encrypts data-at-rest and data-in-motion and conceals the network from unauthorised eyes, thus

enabling compliance to PCI and other payment industry compliance mandates.

Unisys Identity and Access Management

Centrally manages a user's digital identity and their entitlements to provide highest level of identity assurance.

Unisys CyberSecurity Operations Centre

Provides a common operating picture and real-time visibility across all aspects of security operations enabling organisations to implement and conduct IT security that not only protects but also values information.

Unisys Identification and Credentialing

Provides a holistic approach to people identification that combines technology, management, business process and operational expertise to deliver higher levels of identity assurance balanced with trust, privacy and convenience.

Unisys Secure Mobility

Helps organisations improve employee productivity by re-architecting processes for the mobile environment; increase customer engagement with immersive and secure mobile applications; reduce operational cost by enabling users with devices of their choice and manage risk by providing user-based, secured access to corporate asset.

Unisys Secure Cloud

Provides organisations with a pre-integrated solution to deploy, operate and use private clouds. Enterprises can use this solution to transform data centre operations into an agile, efficient and highly automated infrastructure.

About Unisys Security Index

Unisys Security Index is a global study conducted to gauge the attitudes of consumers on a wide-range of security-related issues.

Launched globally in October 2007, it provides a statistically robust measure of concerns around four areas of security – National, Financial, Internet and Personal.

The survey, on which the latest results are based, was conducted nationally between the dates of 2-4 March 2012 by Newspoll and uses a nationally representative sample of 1,206 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data.

Globally the study consists of native-language surveys of 11,093 adults across twelve countries -- Australia, Belgium, Brazil, Colombia, Germany, Hong Kong, Mexico, the Netherlands, New Zealand, Spain, the United Kingdom and the United States -- and provides an overall rating out of 300.

For more information, please visit:
www.unisyssecurityindex.com.au

Contact Information

Media Requests

Julian Brophy, Perception Partners
ph: 02 9699 2722 or 0408 276 749
email: julian@perceptionpartners.com.au

Claire Hosegood, Unisys
ph: 0411 253 663
email: claire.hosegood@au.unisys.com

Briefing Requests

Nick Lake, Unisys
ph: 0424 648 285
email: nick.lake@au.unisys.com