UNISYS

Unisys Security Insights: Australia

A Consumer Viewpoint 2015




How Australian consumers feel about

- Monitoring social media for specific purposes

Research by NEWSPOLL
WHEN THE ANSWER MATTERS

Table of Contents

Executive Summary

Unisys plays a prominent role in efforts to combat risk through the technology products and services it provides to the government and major industries in Australia.

The Unisys Security Insights is a snapshot of the nation's sense of security, and it provides a statistical measure of consumer concerns to enable organisations to make informed security decisions. The research is conducted in Australia by leading market research company NewsPoll.

This study builds on a body of 10 years body of research into the nation's sense of security.

A proactive outlook to security goes beyond bits and bytes, recognizing that the most effective solutions are going to be those formed through collaboration across interests.

See also www.unisys.com/usi-australia

For more information on Unisys security offerings, visit www.unisys.com/security

Unisys Outlook: Public Acceptance of Social Media Monitoring

In 2015 the Australian Unisys Security Insights reveals that the majority of Australians support monitoring social media such as Twitter, Facebook and YouTube to detect possible terrorist activity and to identify public issues and concerns.

The use of social media in coordinating terrorist activity has been widely reported and appears to have had an impact on the Australian public's acceptance of authorities monitoring these channels for public safety and national security purposes.

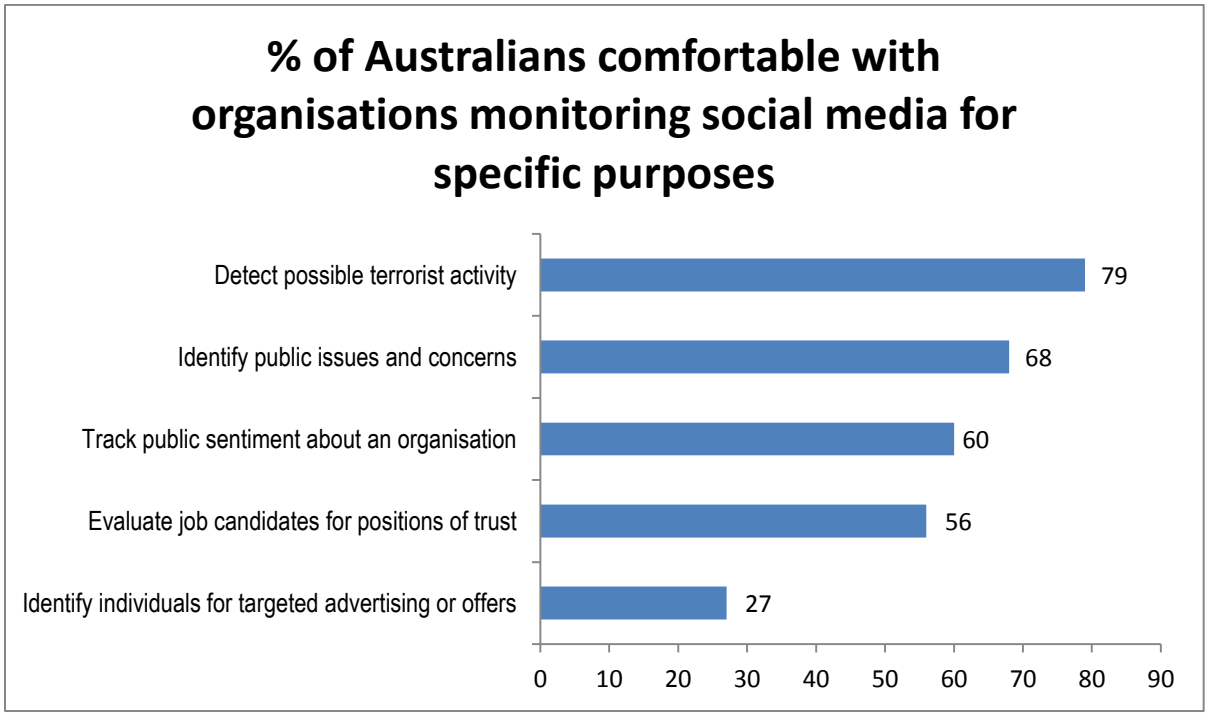
However the extent of Australians' support for social media monitoring varies significantly based on the purpose of the monitoring. There is moderate support for monitoring social media to track an organisation's performance or to evaluate job candidates for positions of trust such as carers or teachers. But there is very little support for using this information for targeted advertising.

These findings serve as a reminder to Australian organisations that they must be clear about why they collect data and how they will protect it, as the public is not comfortable with it being used for a purpose they do not think is necessary.

Results

Detailed Findings: Please say whether you are comfortable or not comfortable with organisations monitoring publically available social media such as Twitter, Facebook and YouTube to do each of the following things?

The majority **79%** of Australians are comfortable with social media monitoring to detect possible terrorist activity



Only 27% support social media morning for targeted advertising or offers

Base = 1210

Level of comfort is fairly even across males and females

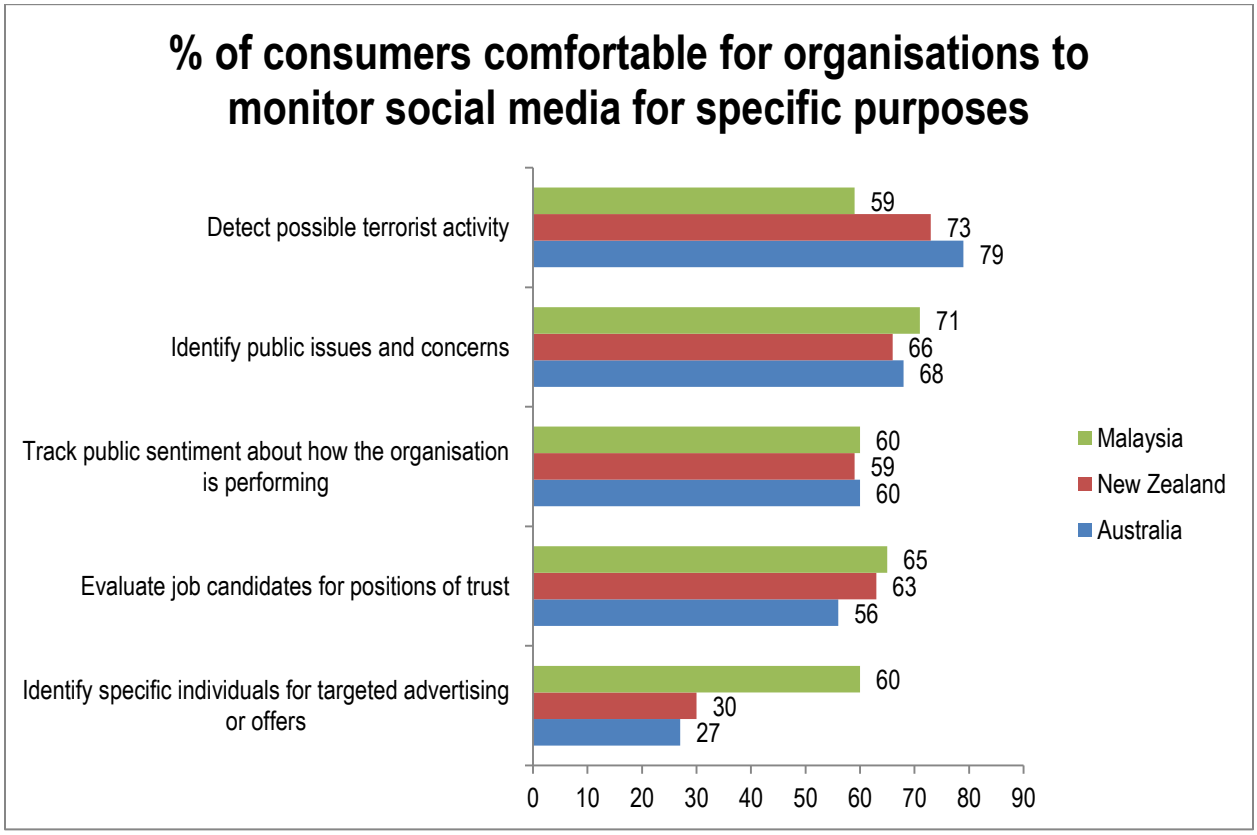
Australians aged under 35 years more comfortable with social media monitoring overall

Younger Australians aged 18-24 years the most comfortable with social media monitoring for targeted advertising and offers

Results

Regional Comparison: Asia Pacific

Public comfort with social media monitoring varies across the region



Detecting possible terrorist activity is ranked the top reason to monitor social media by Australians (79%) and New Zealand (73%), but ranked lowest by Malaysians (59%)

Identifying public issues and concerns is ranked the top reason for social media monitoring by Malaysians (71%)

Identifying individuals for targeting advertising or offers is the least supported reason for social media monitoring by Australians (27%) and New Zealanders (30%), but Malaysians have a high level of comfort (60%) with such monitoring for this purpose

Results

Demographic detail: Australia

% of Australians comfortable for organisations to monitor social media for specific purposes Age Group Comparison

	National	Male	Female	18-24	25-34	Total 18-34	35-49	50-64	65+	Total 50+
Detect possible terrorist activity	79%	80%	78%	83%	84%	76%	70%	73%	79%	86%
Identify public issues and concerns	68%	69%	67%	80%	73%	62%	49%	56%	79%	80%
Track public sentiment about an organisation	60%	62%	58%	74%	67%	53%	36%	45%	78%	72%
Evaluate job candidates for positions of trust	56%	59%	53%	65%	59%	52%	43%	48%	66%	63%
Identify individuals for targeted advertising offers	27%	31%	22%	36%	32%	18%	16%	17%	43%	30%

% of Australians comfortable for organisations to monitor social media for specific purposes State vs State Comparison

	National	NSW/ ACT	VIC	QLD	SA	WA	TAS
Detect possible terrorist activity	**79%**	79%	78%	78%	84%	82%	75%
Identify public issues and concerns	**68%**	68%	68%	65%	68%	73%	66%
Track public sentiment about an organisation	**60%**	59%	58%	61%	59%	64%	63%
Evaluate job candidates for positions of trust	**56%**	56%	56%	52%	62%	59%	55%
Identify individuals for targeted advertising offers	**27%**	25%	28%	32%	21%	24%	23%

Unisys Perspectives on Security

Australians are contributing in a big way to the explosive growth of social media usage – both in terms of sheer volume and the way that we are using it to conduct business. Today we use social media to shop online, book travel, apply for jobs, connect with friends and much, much more. As a result, the amount of personal information available on social media now goes far beyond our Facebook profile.

In the past, social media users enjoyed a sense of anonymity and security due to the large volume of data and the extensive resources that were required for an interested third party to identify, extract and compile personal information spread across billions of pieces of social networking data. However as big data analytics and related technology has improved, the powerful tools needed to analyse the vast amount of social media data have become far less expensive and subscription services have sprung up that put the power of these tools in the hands of even small organisations.

But this survey clearly demonstrates that just because the tools and means exist to do data mining of social media data, that doesn't automatically make it acceptable in the eyes of the Australian public. This research shows that monitoring of social media, even social media in the public domain, raises invasion of privacy concerns in the minds of consumers. And while Australians are generally supportive of relinquishing some privacy in return for personal safety and national security, that doesn't mean they are willing to overlook privacy concerns for the sake of convenience.

Any organisation that collects and maintains personal information regarding their customers needs to exercise great care in protecting that data against misuse or unauthorised access. And this is particularly true when the level of public support suspicion is already high – such as with organisations that mine social network data for non-security related reasons.

Unisys recommends that organisations maintaining personal or sensitive data look beyond traditional security mechanisms to protect against advanced attacks and accidental data disclosures. In particular:

- Converged physical and logical security approach – as logical and physical security measures are converging, leading enterprises across the world should seek ways to solve critical challenges at the point of convergence. Such measures help integrate sensors, consolidate data, provide central or dispersed command and control, use the identity information and support real time as well as offline analytics. Converged security provides seamless monitoring from the "door to the desk" and to the data.

- Biometrics for superior authentication – A robust security strategy incorporates multifactor authentication methods that provide assurance. The authentication can be provided via various biometric techniques like face recognition, DNA matching, fingerprints, voice recognition and vein structure in hands.

  Like organisations, mobile devices too allow for advanced authentication techniques to prevent intrusions and information theft. The opportunity for organisations is to grow in tandem with consumer preferences while ensuring highest levels of protection.

- Isolation and compartmentalisation for data protection – Protecting sensitive information from unauthorised access is the core objective for any security strategy. This typically involves two key activities of identifying the scope of data protection task, and isolating the people, processes and technologies that interact with the sensitive data. Data isolation is achieved by using access controls and encryption to ensure only authorised systems and users can access sensitive information. In addition, compartmentalisation of user groups also result in minimising the threat.

- Comprehensive Security Strategy – Maintaining superior security monitoring, awareness and reporting capabilities within a holistic cybersecurity framework helps protect data and networks from internal and external threats. An all-encompassing security strategy would encompass predictive, preventive, detective and retrospective capabilities.

For information on Unisys security offerings, visit: www.unisys.com/security

Polling methodology

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

Conducted in Australia by market research firm Newspoll the Unisys Security Insights provides a statistically robust measure gauging levels of concern about various aspects of security.

The survey, on which the latest results are based, was conducted nationally in April 2015 by Newspoll using a nationally representative sample of 1,210 respondents aged 18 years and over. All results have been post-weighted to Australian Bureau of Statistics data.

For more information, please visit: www.unisys.com/usi-australia

About Unisys

Unisys is a global information technology company that solves organisations' most pressing IT and business challenges. With more than 20,000 employees serving clients around the world, our offerings include cloud and infrastructure services, application services, business process outsourcing services, and high-end server technology.

We deliver solutions for 10 of top 15 global banks, 15 of top 25 global airlines and more than 200 airlines worldwide. 10 million user incidents are handled in 26 different languages every year and 130 million health and human services transactions are processed each year by Unisys systems. Our processes are end-to-end ITIL v3 compliant and Global ISO 20000, 27001 and 9001 certified. Unisys holds over 1,500 U.S. and non-U.S. patents.

Unisys security offerings are trusted by government and commercial clients around the world to deliver advanced security to counter advanced threats. As logical and physical security threats converge, the world's most important enterprises seek a partner that can bring new ways to solve critical challenges at the point where they converge. Our award-winning, time-tested portfolio of professional services, products, and managed services delivers mission-critical security at scale, helping clients mitigate risk while reducing complexity and cost, and navigating regulatory compliance requirements.

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
Alison Chu, Unisys
email: alison.chu@au.unisys.com