Wallis

WALLIS CONSULTING GROUP PTY LTD
25 KING STREET MELBOURNE 3000 VICTORIA
TELEPHONE (03) 9621 1066 FAX (03) 9621 1919
A.B.N. 76 105 146 174
E-mail: wallis@wallisgroup.com.au

OFFICE OF THE PRIVACY COMMISSIONER, AUSTRALIA

COMMUNITY ATTITUDES TO PRIVACY 2007

prepared for

Office of the Privacy Commissioner, Australia
Level 8, 133 Castlereagh Street
Sydney NSW 2000

August 2007
Reference Number: WG3322

2007 Australian Achiever® AWARDS
Highly Recommended
Excellence in Customer Service
1999-2007 inclusive

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY I

2.0 BACKGROUND INFORMATION 1

2.1 RESEARCH OBJECTIVES 2

3.0 METHODOLOGY 3

4.0 DETAILED FINDINGS 4

5.0 COMMUNITY KNOWLEDGE 5

5.1 AWARENESS OF FEDERAL PRIVACY LAWS 6
5.2 AWARENESS OF THE PRIVACY COMMISSIONER 8
5.3 REPORTING MISUSE OF PERSONAL INFORMATION 9
5.4 KNOWLEDGE OF WHICH ORGANISATIONS ARE COVERED BY THE PRIVACY ACT 11
5.5 KNOWLEDGE OF ACTIVITIES CONTRAVENING THE PRIVACY ACT 14

6.0 TRUST IN ORGANISATIONS 16

6.1 LEVELS OF TRUST IN TYPES OF ORGANISATION HANDLING PERSONAL INFORMATION 17

7.0 INTERACTIONS WITH ORGANISATIONS 21

7.1 TYPES OF INFORMATION RESPONDENTS ARE RELUCTANT TO PROVIDE 22
7.2 REASONS WHY PEOPLE ARE RELUCTANT TO PROVIDE INFORMATION 25
7.3 OMITTING INFORMATION FROM FORMS 26
7.4 AVOIDED DEALING WITH AN ORGANISATION TO PROTECT PERSONAL INFORMATION 27
7.5 ATTITUDES TOWARDS UNSOLICITED MARKETING MATERIAL 29
7.6 ATTITUDES TOWARDS PROVIDING PERSONAL INFORMATION FOR BENEFITS 31

8.0 BUSINESSES AND PRIVACY 33

8.1 USE OF THE ELECTORAL ROLL AND WHITE PAGES FOR MARKETING PURPOSES 34
8.2 MISUSES OF PERSONAL INFORMATION BY BUSINESSES 35
8.3 LEVELS OF CONCERN ABOUT BUSINESS SENDING PERSONAL INFORMATION OVERSEAS FOR PROCESSING 36

9.0 GOVERNMENT DEPARTMENTS AND PRIVACY 38

9.1 ATTITUDES TOWARDS A UNIQUE IDENTIFIER FOR ALL AUSTRALIAN GOVERNMENT DEPARTMENTS 39
9.2 SCENARIOS REGARDED AS MISUSES OF PERSONAL INFORMATION BY GOVERNMENT DEPARTMENTS 42

10.0 HEALTH SERVICES AND PRIVACY 44

10.1 ATTITUDES TOWARDS INCLUSION IN A NATIONAL HEALTH DATABASE 45
10.2 ATTITUDES TOWARDS HEALTH PROFESSIONALS SHARING PATIENT INFORMATION 47
10.3 ATTITUDES TOWARDS DOCTORS DISCUSSING PERSONAL MEDICAL INFORMATION IN AN IDENTIFIABLE WAY 48
10.4 ATTITUDES TO THE DISCLOSURE OF THE FACT THAT A PATIENT HAS A GENETIC ILLNESS - WITH AND WITHOUT CONSENT 49

TABLE OF CONTENTS Cont'd

11.0 PRIVACY IN THE WORKPLACE 51

11.1 EMPLOYEES' ACCESS TO INFORMATION EMPLOYERS KEEP ABOUT THEM 52
11.2 ATTITUDES TOWARDS EMPLOYERS READING EMAILS, DRUG AND ALCOHOL TESTING AND MONITORING VEHICLE LOCATIONS 55
11.3 ATTITUDES TOWARDS EMPLOYERS USING SURVEILLANCE EQUIPMENT TO MONITOR THE WORKPLACE 57
11.4 ATTITUDES TOWARDS EMPLOYERS MONITORING TELEPHONE CONVERSATIONS 58
11.5 IMPORTANCE OF EMPLOYER PRIVACY POLICIES 59

12.0 PRIVACY AND THE INTERNET 60

12.1 LEVELS OF CONCERN ABOUT PERSONAL INFORMATION ON THE INTERNET 61
12.2 PROVIDING FALSE INFORMATION ONLINE AS A MEANS OF PROTECTING PRIVACY 64
12.3 USE AND IMPACT OF PRIVACY POLICES ON ATTITUDES TO WEBSITES 65

13.0 IDENTITY FRAUD 66

13.1 INCIDENCE OF ID FRAUD AND THEFT 67
13.2 ACTIVITIES THAT MOST EASILY ALLOW IDENTITY FRAUD OR THEFT TO OCCUR 69
13.3 SHOWING AND COPYING IDENTIFICATION DOCUMENTS 71

14.0 PRIVACY IN PUBLIC PLACES – CCTV 73

14.1 AWARENESS AND CONCERNS ABOUT CCTV 74
14.2 ACCESS TO CCTV FOOTAGE 76
14.3 APPROPRIATE POSITIONING OF CCTV CAMERAS 78

APPENDIX 1: VERIFICATION STUDY 80

APPENDIX 2: QUESTIONNAIRE 83

1.0 EXECUTIVE SUMMARY

Wallis Consulting Group was commissioned by the Office of the Privacy Commissioner, Australia (the Office) to conduct the 2007 Community Attitudes Towards Privacy Study. The study aims to understand Australians' changing awareness and opinions about privacy laws, how they apply to government and business and how individuals view a range of emerging issues, in particular, identity fraud and theft and the use of closed circuit television.

As was the case in previous studies undertaken by the Office in 2001 and 2004, the 2007 study was conducted by telephone. 1503 respondents were selected at random from an electronic listing of home telephone numbers. Quotas were placed on the number of interviews conducted by age and location and the data set was then weighted to reflect the characteristics of the adult Australian population as measured in the 2006 Census by the Australian Bureau of Statistics.

In comparison with 2004, community attitudes have changed significantly in the following areas:

- Public trust in the ability of organisations to handle personal information appropriately has increased for health service providers, and Government departments. It has declined for financial institutions and has remained stable for charities, retailers, market research organisations and businesses selling over the Internet.
- An increasing proportion of Australians are willing to provide a wide range of personal information to organisations. Whereas, in 2004, 58% were reluctant to provide financial information, now only 43% are reluctant. While the proportion of respondents reluctant to divulge their financial details in general has declined, the proportion saying they are **most** reluctant to release salary details has doubled to 18%.

  One of the largest changes is the fall in the proportion of Australians who say they are reluctant to disclose health information. Only 6% of Australians are reluctant to provide this information now, compared with 21% in 2004.

  The reasons Australians are reluctant to release information remain the same - most feel that organisations have no right to know this information or that it might lead to unwelcome unsolicited direct marketing activity by mail or telephone. A smaller proportion is concerned that providing this information may lead to financial loss via unsolicited access of their bank accounts or other crime.

- The proportion of Australians willing to provide personal information if they have a chance of gaining a discount declined. Now 22% say they are likely to give personal information for a discount, compared with 28% in 2004. Only 14% of Australians would be motivated to give information in exchange for a prize.
- There has been a slight increase, to 36%, of respondents who have decided not to deal with a business or charity because of concerns over the way that organisation might handle their personal information. The proportion that has avoided Government departments on the same grounds (12%) is lower than when measured in 2004 (16%).
- The number of people who believe the Electoral Roll should not be used for marketing purposes has increased from 77% in 2004 to 82% in 2007. Support for using the White Pages for marketing purposes is increasing, with 46% in favour. While the increase is not significant compared with 2004, it is when compared with 2001 when 42% agreed. Nonetheless, 50% do not agree with using the White Pages for marketing purposes.
- The community's reactions to being sent unsolicited marketing information are gradually becoming less favourable. Receiving this material continues to cause 53% of recipients to wonder from where the sender obtained their details. An increasing proportion, currently standing at 27%, feel angry and annoyed by it. Only 4% welcome its arrival and enjoy reading it compared with 7% in 2004 and 9% in 2001.
- Community support for a unique identifying number to be used by Australians accessing Government services has increased in the last three years to 62% (up from 53% in 2004). Support for Government departments being able to cross reference or share information has increased from 71% in 2004 to 80%. Australians support sharing information most if it is for the purpose of solving fraud or other crime (77%), or for updating information (67%). When asked if they considered it appropriate to share information on the grounds of increased efficiency, 49% agreed.
- Seventy six percent (76%) of Australians felt that inclusion in a national health database should be voluntary compared with 64% in 2004. The community was evenly divided on whether or not de-identified information from this database should be made available for research purposes.
- Fifty percent of respondents said they were more concerned about providing information over the Internet than they were two years ago. Generally speaking, the community is more concerned about providing information over the Internet than in hard copy format or over the telephone. Despite this, 67% of Australians claimed not to provide false information over the Internet in order to protect their privacy.

- Australians are now more aware both of the existence of privacy laws and of the Office. Sixty nine percent (69%) of Australians are aware of the laws now (up 10%) and 45% are aware of the Commissioner (compared with 34% three years ago). However, the community remains unsure as to the extent of coverage of the Privacy Act, with most correctly nominating that it covers government and big business. Significant proportions also believe it applies to state government, small businesses and businesses domiciled overseas. The majority correctly believes that the Act relates to correct handling of personal information. Over half also believe that some matters relating to personal privacy, for example their neighbours spying, are also included.

In general terms, attitudes were stable regarding matters relating to privacy in the workplace and the release of medical details. In particular:

- Eighty six percent (86%) of Australians continue to think that employees should have access to information that employers keep about them. Most also believe that employers are entitled to monitor employees' emails, computers, telephone conversations and their whereabouts, as well as undertaking surveillance activities and random drug and alcohol testing in certain circumstances – especially where wrongdoing is suspected, for the safety and security of employees or, in the case of monitoring telephone conversations, for the purposes of training and quality control. Depending on the activity, between 20% and 30% of Australians believe that employers should not be able to undertake these at all.
- Sixty percent (60%) of Australians continue to support their doctor discussing their own personally identified medical details with other health professionals.

However on the subject of informing relatives about the presence of a genetic illness – a new area of investigation for this survey – a slim majority (55%) believes that this should be done without the patient's consent. Of these, 36% believe this should be done only if there is a strong possibility that the relative may have the illness, and 19% think it should be done irrespective of the likelihood of the illness being inherited. Forty three percent believe relatives should only be told if the patient consents to it.

Other new topics were discussed with respondents in this study:

- The majority of Australians (90%) are concerned about businesses sending their personal information overseas, with 63% being *very concerned.*
- While 9% claim to have been the victim of identity fraud or theft, 17% claim to know someone who has been. People aged between 35 and 49 are the most likely to have been the victim or know someone who has been. Western Australians also displayed a significantly higher incidence (14%) of being a victim than others. This question was also included in the Verification Study conducted by NewsPoll and exactly the same results were obtained. Sixty percent (60%) of Australians are concerned that they may become a victim.
- The most likely way that identity fraud and theft can occur is considered to be the Internet – a view held by 45% of the community. Losing identifying documentation through carelessness or theft, or losing sight of credit cards are also considered to be major contributors.
- Over 80% of Australians believe it is reasonable to show identifying documentation to gain access to licenced premises, but only 18% think it is reasonable to have their documentation copied. Support is high for showing documentation to obtain a credit card (96%), and to purchase goods for which an individual must be aged over 18 (93%). While 57% still think it reasonable to have identifying documents copied in order to obtain a credit card, support drops to less than 23% in the other cases.
- Most Australians are aware of CCTV and the majority is not concerned about its use. Concerns mostly relate to the potential misuse of captured footage and a perceived invasion of privacy. Even those who were concerned suggested people and organisations who should have access to the footage and places where they felt it appropriate for CCTV cameras to be placed. Amongst those aware of cameras, 88% felt it reasonable for the police to have access to footage. Other organisations received lower levels of support for having access, with 20% nominating security companies, 15% the government, 13% anti-terrorist agencies and 11% the company that installed the camera.

- While 9% of Australians were happy to have CCTV cameras placed anywhere (with the exception of public toilets and changing rooms), the majority are happy with public places. Private institutions including banks, entertainment venues, pubs and clubs were nominated by 29%. Of the people aware of CCTV cameras, 8% supported placing cameras in public institutions including government offices, hospitals, schools and police stations.

2.0 BACKGROUND INFORMATION

The Office of the Privacy Commissioner, Australia (the Office) is an independent statutory body that operates with the purpose of promoting and protecting privacy in Australia. The Office has responsibilities under the *Privacy Act (1988)* for the protection of individuals' personal information handled by Australian and ACT Government departments, large businesses and some small businesses. Australian and ACT Government departments have been covered by the Information Privacy Principles since 1989 and most private sector organisations have been covered by the National Privacy Principles since 2001.

The Office has undertaken regular studies to understand community attitudes towards privacy in Australia since the early nineties. The two most recent studies, conducted in 2001 and 2004[1], adopted very similar lines of questioning and, with the extension of the Privacy Act to include the private sector, sought to understand public awareness of the legislation and its rights under it. In 2001 the key focus of the study was to provide information about community attitudes towards privacy generally. The focus shifted in 2004 to provide input into a review of the private sector provisions of the Privacy Act.

[1] Roy Morgan Research

2.1 RESEARCH OBJECTIVES

The principal research objectives of the 2007 Community Attitudes Survey are to gauge public opinion and awareness on a range of issues relating to the use and handling of personal information by business and government organisations.

The objectives for the 2007 study are:

1. To provide input into the Office's response to the Australian Law Reform Commission's forthcoming Discussion Paper on its review into privacy legislation.
2. To assist in the Office's policy and compliance work, particularly in informing thinking on various issues.
3. To inform the Office's communications work, particularly in identifying issues and audiences that require a focussed response or level of pro-activity in terms of the Office's educational work.
4. To provide information on privacy trends and developments for the Office's stakeholders.
5. To track changes in community attitudes since the last research and to use this information as a benchmark for future studies.

3.0 METHODOLOGY

Data for this study was collected through Computer Assisted Telephone Interviewing between 11 July and 7 August 2007. All calls were made from Wallis Consulting Group's Telephone interviewing facility in Melbourne. In total 1503 interviews were completed with a representative sample of Australians. In order to ensure that the responses of younger Australians could be compared with those aged over 25, this population group was over sampled. The data was then weighted to match 2006 Australian Bureau of Statistics population Census data on the basis of age, sex and location of respondents. The interview took, on average, 27 minutes for respondents to complete. The questionnaire used is found at Appendix 2. The full methodology used to conduct this study is published separately.

Table 1. Number of interviews completed by age, sex and location.

Sex	Age	Total	SYD	NSW/ ACT	MEL	VIC	BRIS	QLD	ADEL	SA/ NT	PERTH	WA	TAS
Male	18-24	**74**	12	13	27	3	8	4	3	0	3	0	1
Male	35-49	**194**	55	29	34	12	11	19	6	7	11	5	5
Male	50+	**245**	51	36	24	22	20	25	20	10	24	7	6
Female	18-24	**91**	15	10	29	1	8	11	4	0	10	3	0
Female	25-34	**222**	45	29	50	11	24	25	8	5	14	5	6
Female	50+	**288**	47	46	34	20	24	28	30	13	23	10	13
Total		**1503**	**315**	**210**	**270**	**90**	**135**	**150**	**90**	**48**	**105**	**45**	**45**

In addition to the main study a verification study was conducted in which three questions from the main study were asked on the NewsPoll Omnibus and the results compared. The results from this study are included at Appendix 1.

4.0 DETAILED FINDINGS

This report provides a descriptive analysis of each survey question and includes comparisons to the previous community attitudes to privacy survey results (2001, 2004 and studies undertaken in the early 1990s) where applicable. Results shown are by age, gender, location, combined household income, highest achieved level of education and occupation, where significant differences in opinion occurred. Differences noted are significant to the 95% confidence limit.

The topics examined in this survey include:

- Community knowledge and awareness of privacy issues
- Trust in organisations' handling of personal information
- Attitudes towards business' handling of personal information
- Attitudes towards government departments' handling of personal information
- Health services and privacy
- Privacy in the workplace
- Privacy and the Internet
- Identity fraud and theft
- Privacy in public places – closed circuit television (CCTV)

5.0 COMMUNITY KNOWLEDGE

In order to protect Australians' personal information it is important that the community know that they have rights pertaining to the handling and use of their personal information, that they know what those rights are and how to exercise them. The extent to which the community is aware of these fundamental aspects of privacy is addressed in this section.

Community knowledge of privacy laws was ascertained, as in previous surveys, by asking respondents questions about their awareness of their existence; whether they were aware that there is a Federal Privacy Commissioner; where they would go to report misuse of their personal information; whether certain organisations are bound by Privacy Laws; and, additionally in 2007, whether or not they considered certain activities to be contraventions of the *Privacy Act 1988*.

5.1 AWARENESS OF FEDERAL PRIVACY LAWS

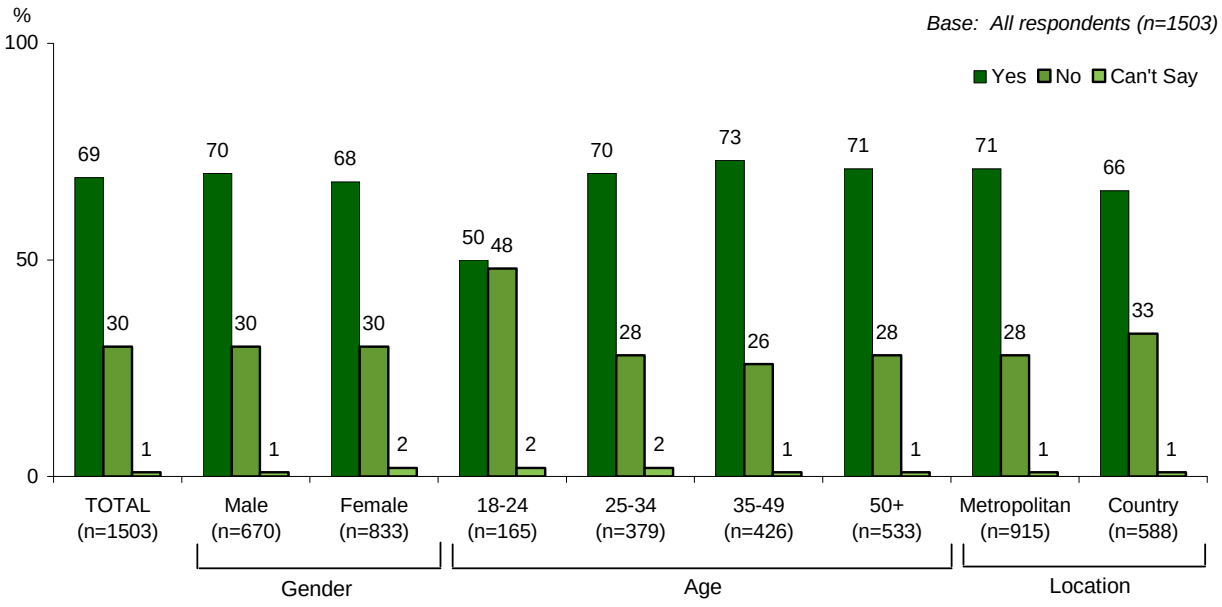
Sixty-nine percent of respondents said they were aware that Federal privacy laws existed. Awareness has almost doubled since first measured in 1994 (36%). They have increased significantly every time they have been measured since (43% in 2001, 60% in 2004).

Chart 1 and Table 2 demonstrate that:

- Increases in awareness occurred in all states in comparison to 2004. Western Australia continued to record significantly lower levels of awareness at 58% compared to other states.
- Younger respondents continue to be less aware of privacy laws than older respondents. Those aged 18-24 (50%) had similar levels of awareness to those recorded in 2004 (48%), while awareness amongst other age groups continued to increase.

Respondents who had achieved higher levels of education were more likely to be aware of the privacy laws. For example 59% of people educated up to Year 12 were aware, compared with 80% of people who are tertiary educated.

Chart 1. Awareness of Federal privacy laws



Q. Were you aware of the Federal PRIVACY LAWS before this interview?

Table 2. Awareness of Federal privacy laws by state

	2001 (n=1524) %	2004 (n=1507) %	2007 (n=1503) %
NSW	44	**61**	**71**
VIC	40	**63**	**70**
QLD	43	**59**	**69**
WA	51	51	58
SA*/NT	38*	**61**	69
TAS	42	**63**	66

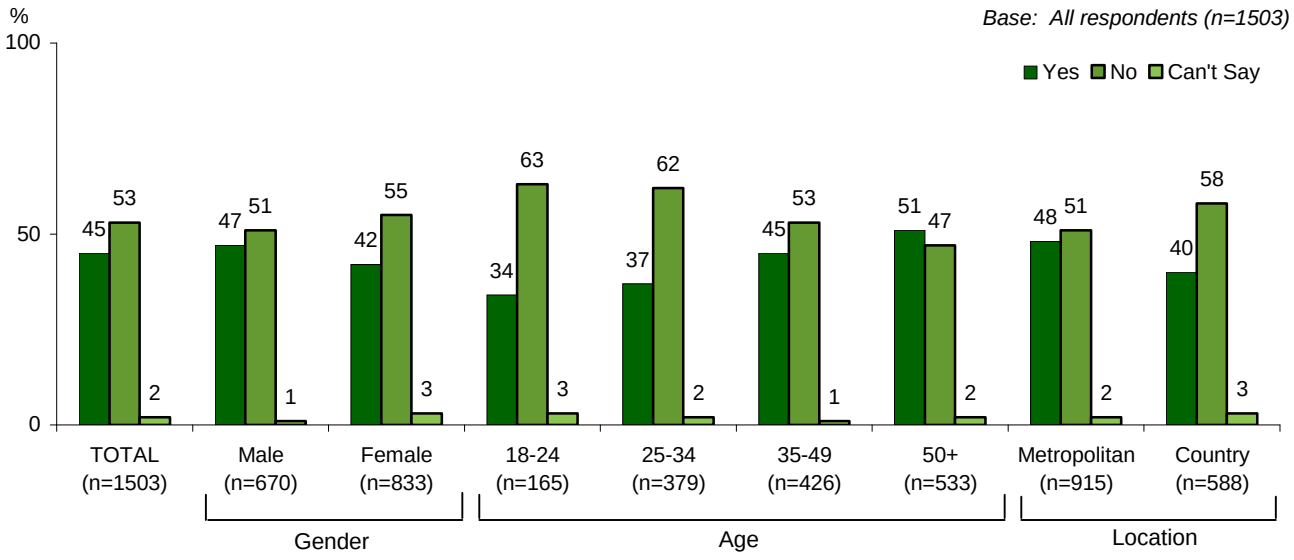
**SA only, awareness in NT was 40%*
Base sizes vary within each state by year
Bold indicates a significant increase on the previous year

5.2 AWARENESS OF THE PRIVACY COMMISSIONER

Awareness of the Privacy Commissioner continues to increase. It now stands at 45% of Australians saying they are aware, in comparison with 36% in 2001 and 34% in 2004. Awareness is highest in Victoria (49%), Tasmania (49%), NSW (48%), South Australia (46%) and the Northern Territory (46%) and at the same lowest level in Western Australia and Queensland (both 36%). In 2004 in South Australia and the Northern Territory, awareness was lower relative to the other states, however, awareness is now on par with the national average.

Respondents who live in metropolitan areas (48%) were more likely to be aware than those living elsewhere (40%). Awareness increases with increasing age (see Chart 2)

Chart 2. Awareness of Federal Privacy Commissioner



Q. Are you aware that a Federal Privacy Commissioner exists to uphold privacy laws and to investigate complaints people may have about the misuse of their personal information?

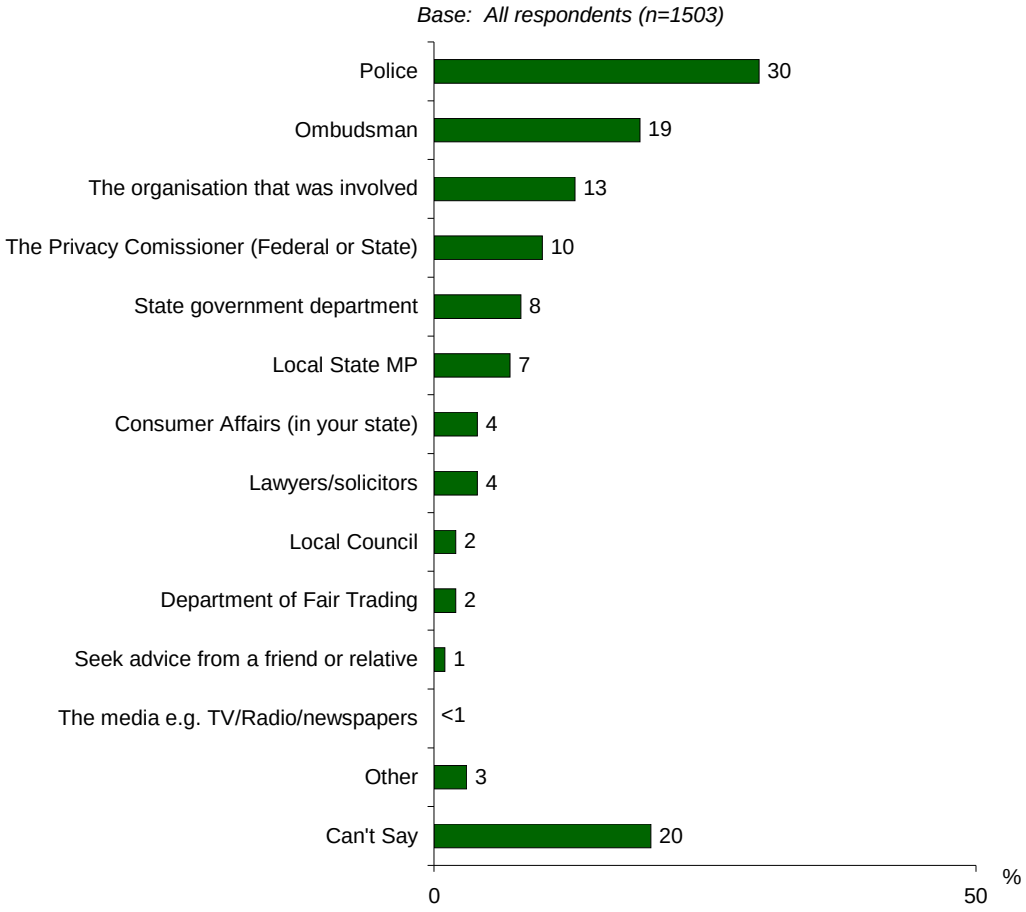
5.3 REPORTING MISUSE OF PERSONAL INFORMATION

Respondents were asked who they would contact if they wanted to report misuse of their personal information. The results indicate increasing confidence in knowing how to make a report, demonstrated by the lower proportion unable to name an appropriate person or organisation. Nonetheless, 20% (down from 29% in 2004) could not answer the question.

The *police* were mentioned by 30% as the organisation they would contact. This is a significant increase compared with 2004 when 13% nominated *the police*. The *Ombudsman* was mentioned by 19%, and 13% said they would go to *the organisation involved*. One in ten (10%) respondents said they would go to a *privacy commissioner,* compared with 7% in 2004 and 5% in 2001. The following differences were observed:

- NSW Respondents (14%) were more likely than those from other states to go to a *privacy commissioner*. Queenslanders and Tasmanians were the most likely to go to *the police* (37% and 39% respectively) and Tasmanians (33%) were also more likely to go to an *ombudsman*.
- Those living in metropolitan areas (13%) were more likely to go to a *privacy commissioner* than those living elsewhere (7%).
- Australians aged between 18-24 (38%) were more likely than those aged over 50 years (28%) to report a misuse to *the police*, while those aged over 35 years were more likely than younger Australians to say they would go to an *ombudsman*.
- Those with tertiary level qualifications are more likely to go to a *privacy commissioner* (18%) or an *ombudsman* (24%) while those who have up to a Year 12 equivalent education (35%) are more likely to go to *the police.*

Chart 3. Reporting misuse of personal information



Q. If you wanted to report the misuse of your personal information, who would you be most likely to contact?

5.4 KNOWLEDGE OF WHICH ORGANISATIONS ARE COVERED BY THE PRIVACY ACT

The *Privacy Act (1988)* applies to:

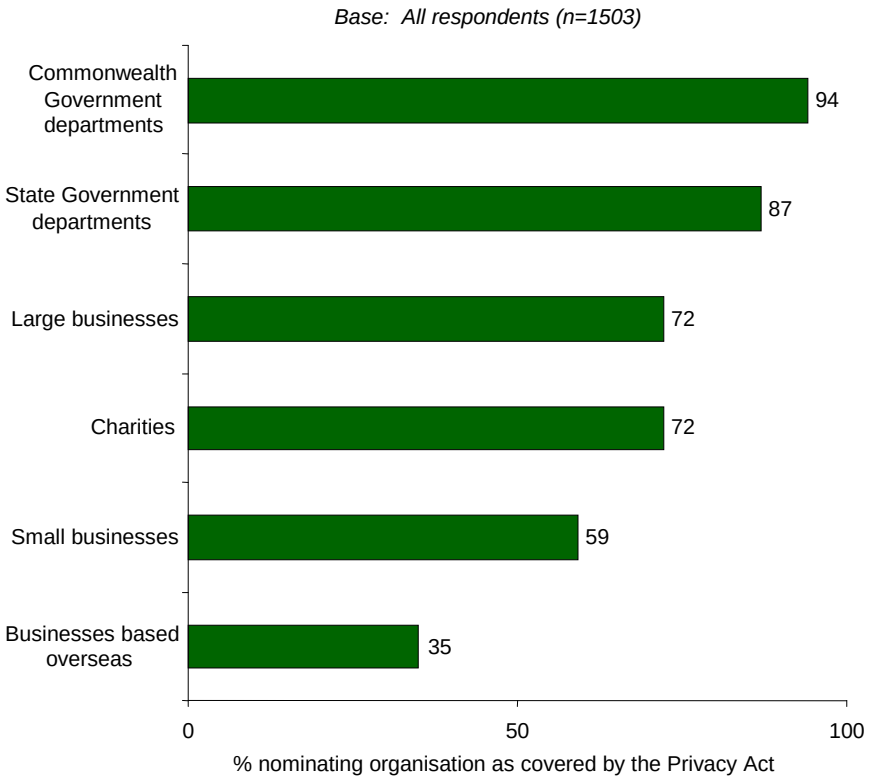
- Australian and ACT Government departments;
- businesses with a turnover of more than $3M; and
- small businesses that are health service providers, trade in personal information, are related to a business that is not a small business or are contractors providing services under a Commonwealth contract.

State Government departments are not covered by the Privacy Act, neither are most small businesses or businesses based overseas. Awareness of which organisations are generally covered by the Federal Privacy Act is covered in this section[2].

[2] As the corresponding questions were asked in a significantly different manner in 2004 it would not be appropriate to make a comparison in this report.

Respondents were read a list of organisations and asked which ones they believe are covered by the Privacy Act.

Chart 4. Knowledge of which organisations are covered by the Privacy Act



Q. I'm going to list six types of organisations. Which of these, if any, do you think GENERALLY must operate under the Federal Privacy Act?

The vast majority of respondents correctly nominated Commonwealth Government departments (94%) as well as large businesses and charities (72%). Most (87%) perceive State Government departments and small business (59%) to be covered by the Privacy Act. Most were correctly aware that businesses based overseas are not covered, however 35% incorrectly thought them to be.

Australians aged up to 24 years were more likely to believe that the Privacy Act applies to all organisations. With the exception of businesses based overseas, those aged over 50 years were less likely to think organisations were covered.

Lower blue collar workers were more likely to believe that the Privacy Act is more comprehensive in its coverage than other respondents. Of these, 94% nominated *State governments* and 52% thought that *businesses based overseas* were covered. They were also more likely to nominate large business (81%) than were other respondents.

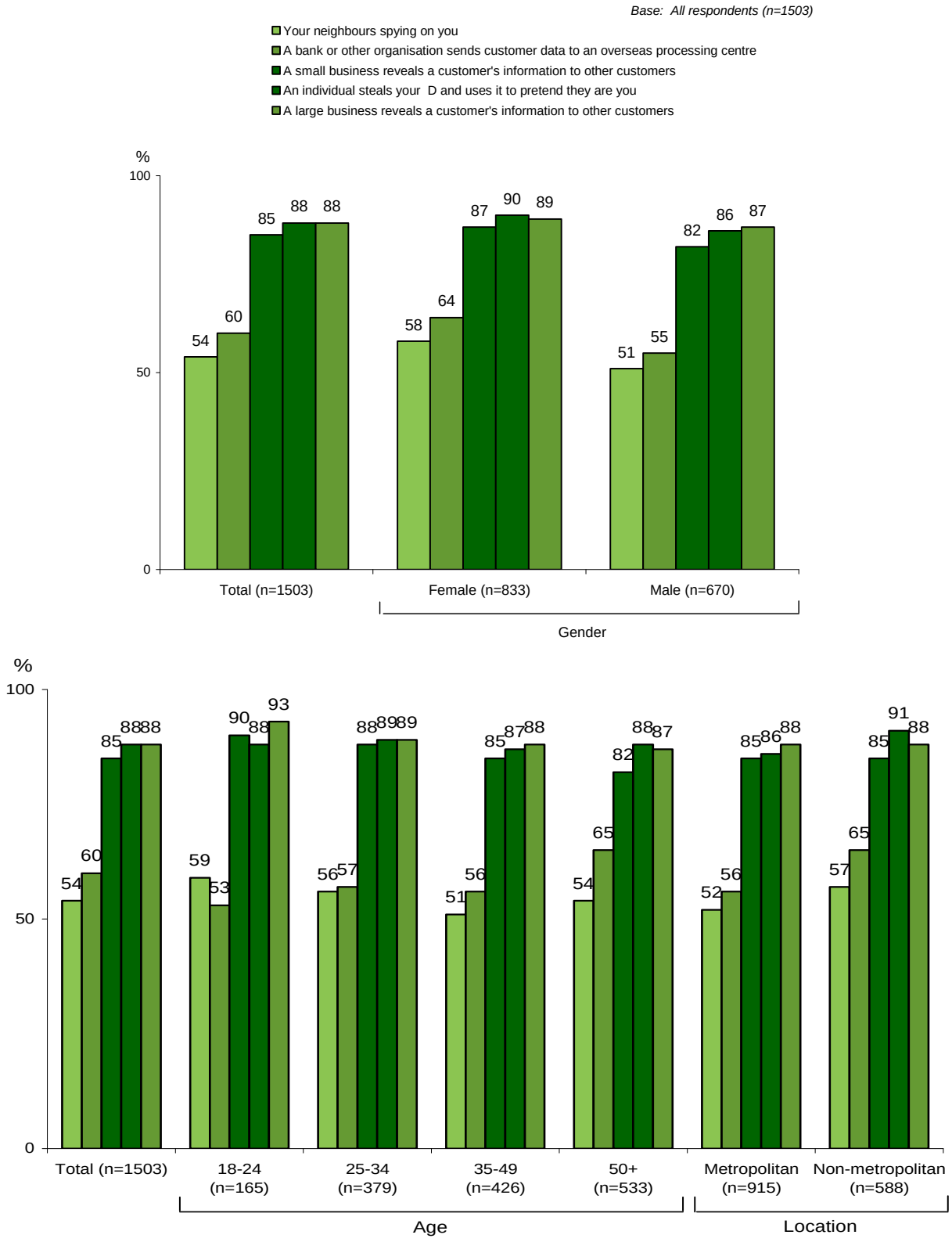
5.5 KNOWLEDGE OF ACTIVITIES CONTRAVENING THE PRIVACY ACT

The Privacy Act covers the collection, storage, access and transfer of personally identified information on private individuals. Respondents were asked whether or not certain activities undertaken by different types of people or organisations were against the Privacy Act. The majority (88%) correctly, were of the opinion that *ID theft* and *revealing customer information* – by large (88%) or small (85%) business – contravenes the Privacy Act. *Spying by neighbours* was incorrectly thought to be a contravention by 54% and 60% thought that *a bank sending customer information overseas* was a violation of the Act.

Chart 5 shows that women were more likely than men to think that all these activities contravened the Act. In addition:

- Those aged over 50 years (65%) were more likely than those under 50 (18-24 – 53%, 25-34 – 57% and 35-49 – 56%) to believe that *a bank sending customer information overseas* contravenes the Act.
- Those with a tertiary education were less likely than average to believe that *spying* (44%) or *sending information overseas* (48%) contravene the Act.

Chart 5. Activities respondents feel contravene the Privacy Act – By sex, age and location



Q. Which of the following activities, if any, would be against the Federal Privacy Act?

6.0 TRUST IN ORGANISATIONS

As in previous surveys, respondents were asked to rate the trustworthiness of certain organisations[3] in regard to the protection of their personal information. Including:

- Financial institutions;
- Real estate agents;
- Charities;
- Government departments;
- Health service providers including doctors, hospitals and pharmacists;
- Market research organisations;
- Businesses selling over the Internet;
- Retailers; and
- Insurance companies (included for the first time in the 2007 survey).

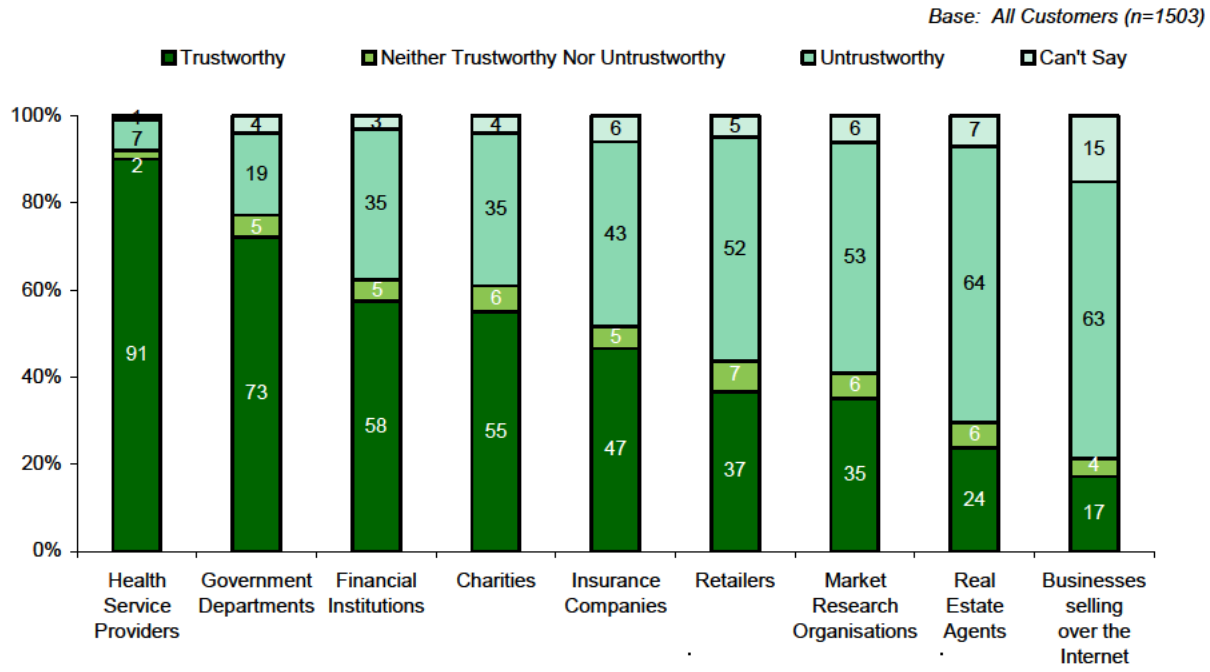
[3] Mail order companies were excluded from the 2007 survey.

6.1 LEVELS OF TRUST IN TYPES OF ORGANISATION HANDLING PERSONAL INFORMATION

Perceived trustworthiness, in regard to the protection of personal information, has increased for *Health Service Providers* and *Government departments* in comparison with 2004. It was stable for *charities*, *market research organisations* and *real estate agents* and it declined for *financial institutions.*

Health Service Providers are trusted most (91%), with lower levels of trust associated with Government departments (73%), financial institutions (58%) and charities (53%). Other organisations elicited higher levels of mistrust than trust.

Chart 6. Trust in organisations handling personal information



Q. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information?

6.1.1 Health Service Providers

There has been a steady increase in the proportion of respondents who say they trust Health Service Providers during the survey periods (91% in 2007, 89% in 2004, 84% in 2001 and 70% in 1994). Health Service Providers are believed to be trustworthy by 91% of Australians. Australians who hold tertiary qualifications (88%) are less likely to feel that Health Service Providers are trustworthy than those educated up to Year 12 (92%).

6.1.2 Government departments

There has been a significant, positive shift in attitudes towards government departments since 2001. Government departments are believed to be trustworthy by 73% of Australians, compared with 64% in 2004 and 58% in 2001. Government departments are now perceived to be more trustworthy than financial institutions. As age increases the degree of trust in government departments decreases, with 87% of 18 – 24 year olds finding them trustworthy, compared with 67% of Australians aged over 50.

6.1.3 Financial institutions

Levels of trust in financial institutions declined from 66% in 2004 to 58% in 2007. The current level of trust is at similar levels to those measured in 2001 (59%). Regardless of the decline, financial institutions remain among the most trusted types of organisations. 18-24 year olds (73%) are more likely than those aged over 50 years (50%) to say that financial institutions are trustworthy. Retirees (48%) are less likely to trust financial institutions than those who are working (60%).

6.1.4 Charities

The level of trust in charities remains stable at 55%. However 69% of Australians aged 18-24 were the most likely to trust them, compared with 47% of Australians aged over 50. Tasmanians (67%) were also more likely to trust charities in handling personal details compared with Australians living elsewhere.

6.1.5 Insurance companies

Whereas 47% of Australians thought insurance companies could be trusted with personal information, trust decreases with increasing age, with 55% of 18-24 year olds finding them trustworthy compared with 41% of Australians aged over 50.

6.1.6 Retailers

Trust in retailers' handling of personal information has remained stable over the course of the surveys. In 2007, 37% thought retailers were trustworthy, compared with 39% in 2004 and 36% in 2001. Trust in retailers is greater amongst people living in non-metropolitan areas (42%). Education is also a factor, with a lower proportion of those holding a tertiary qualification (31%) trusting retailers, compared with those educated up to Year 12 (42%).

6.1.7 Market research organisations

There was no difference in perceived levels of trustworthiness of market research organisations between 2004 and 2007 (35%). Levels of trust remain higher than they were in 2001 (32%) and 1994 (29%). Western Australians (42%) and Tasmanians (46%) were more likely than those from NSW (32%) and Victoria (32%) to think market research organisations are trustworthy. Queenslanders (37%) and South Australians (36%) were close to the national average (35%).

6.1.8 Real estate agents

There continues to be a low level of trust within the community in real estate agents' handling of personal information, with only 24% saying they are trustworthy. Although this is the same as 2004 (26%), it remains higher than 2001 results (20%).

6.1.9 Businesses selling over the Internet

Businesses selling over the Internet continue to be perceived as the least trustworthy of the organisations considered by respondents. While only 17% considers these to be trustworthy, it is a significant improvement on 2004 (9%).

7.0 INTERACTIONS WITH ORGANISATIONS

The exchange of personal information between individuals and organisations occurs when interactions take place, whether initiated by the individual or the organisation. This section examines some of the issues around these interactions. Topics examined are:

- types of information that people are reluctant to provide;
- omitting information from forms;
- decisions about dealing with organisations on the basis of their handling personal information;
- attitudes towards unsolicited marketing material; and
- attitudes towards providing personal information in exchange for benefits.

7.1 TYPES OF INFORMATION RESPONDENTS ARE RELUCTANT TO PROVIDE

Respondents were asked which types of information they are, in general, reluctant to provide. As was the case in 2001 and 2004 they were most reluctant to provide *financial details* and *details about income*, followed by *contact details*. However, there was a decline in the proportion that were reluctant to provide *financial details* (43% in 2007 versus 58% in 2004).

Compared with 2001 and 2004, Australians were far less likely to say that they are reluctant to provide their *medical history/health information*. This large shift, from 21% in 2004 to 6% now may be related to the increasing level of trust Australians have in health service providers' ability to manage their personal information (see section 6.1.1). To a lesser extent, there was also a decline in reluctance to provide *email addresses*, *genetic information* or *a name*.

Table 3. Types of information Australians are reluctant to provide

Type of information	2001 (n=1524) %	2004 (n=1507) %	2007 (n=1503) %
Financial details	59	58	*43*
Details about income	42	34	34
Home phone number	17	22	**25**
Home address	14	20	19
Email address	11	19	*14*
Date of birth	7	8	**10**
Marital status	9	9	*7*
Medical history/health information	25	21	*6*
Genetic information	13	11	*5*
Name	6	7	*4*
How many people or males in the household/ family member details	1	2	**4**
Religion	2	3	2
Drivers licence	-	-	1
Occupation	-	-	1
Other	-	-	4
Depends	-	-	2
None	16	11	10

Base: all respondents
Bold denotes a significant move up, italics a significant shift down between 2007 and 2004
Note: answers add up to more than 100 as multiple responses were given

Q. When providing your personal information to any organisation, In general, what types of information do you feel reluctant to provide?

Respondents were asked which **one** type of information they are *most* reluctant to provide. Their answers are shown in Table 4.

Table 4. Type of information MOST reluctant to provide

Type of information	2001 (n=1524) %	2004 (n=1507) %	2007 (n=1503) %
Financial details	40	41	*35*
Details about income	11	10	**18**
Home phone number	3	5	**9**
Home address	4	7	7
Email address	2	5	5
Date of birth	1	1	**3**
Medical history/health information	7	5	*2*
How many people or males in the household/ family member details	<1	<1	**2**
Genetic information	3	2	*<1*

Base: all respondents
Bold denotes a significant move up, italics a significant shift down between 2007 and 2004

Q. And of [LIST ANSWERS PROVIDED] which one of these do you feel most reluctant to provide?

Financial details were still nominated by 35% of respondents, a lower proportion than in 2004. However, 18% nominated *details about income* – an 8% increase from 2004.

Differences in opinion were observed between:

- People living in households earning more than $100,000 (19%) are the most likely to be reluctant to provide *details about their income* (cf. 11% of those living in households earning less than $25,000). However, these groups share a similar level of concern about providing their *financial details* (less than $25,000 – 34%, and greater than $100,000 – 31%).
- Those living in metropolitan areas (31%) are less concerned about providing their *financial details* than those living elsewhere (40%).

As was the case in 2004, Australians' concerns about providing financial details increased with increasing age. Conversely, younger Australians are the most concerned about releasing their home phone number or home address.

7.2 REASONS WHY PEOPLE ARE RELUCTANT TO PROVIDE INFORMATION

For most, the principal reason for not wanting to provide personal details is that *it is none of their business* (36%). Following this are the potential for *financial loss* (14%), *becoming the victim of crime* (12%), or *being subjected to marketing activity* (via telephone or in person) (12%).

Table 5. Reasons for being reluctant to provide information

Reasons for being reluctant to provide information	2001 (n=1306) %	2004 (n=1294) %	2007 (n=1305) %
It's None of Their Business / Invasion of Privacy	51	44	*36*
May Lead to Financial Loss / People Might Access Bank Account	7	8	**14**
For Safety / Security / Protection (From Crime)	2	6	**12**
I Don't Want to Be Bothered/ Hassled / Hounded (by Phone / Door to Door)	1	5	**12**
The Information May Be Misused	12	8	**11**
Don't Want Junk Mail / Unsolicited Mail / Spam	1	5	**11**
Unnecessary / Irrelevant to Their Business or Cause	2	5	**9**
I Do Not Want People Knowing Where I Live/ How to Contact Me	6	5	5
Information Might Be Passed on Without my Knowledge	5	3	**5**
Discrimination	4	3	*2*
I Do Not Want to Be Identified	3	1	**2**
Other	3	3	*2*
Can't Say	4	2	*1*

Base: reluctant to provide information

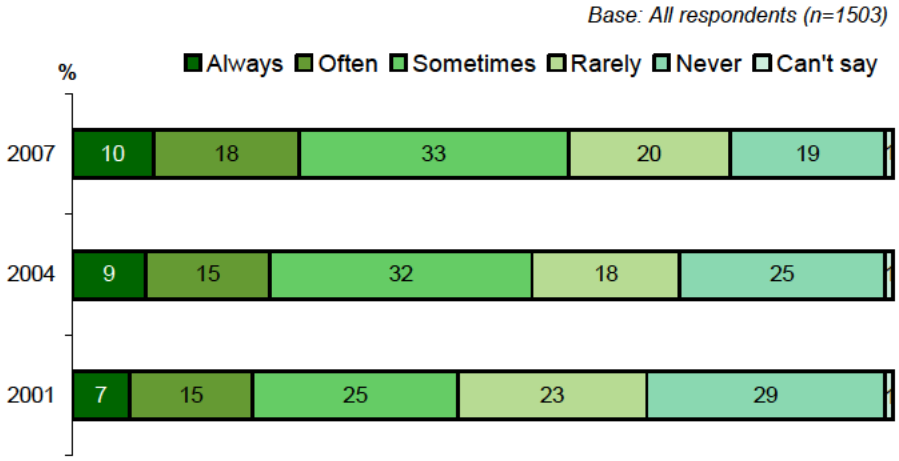
Bold denotes a significant move up, italics a significant shift down between 2007 and 2004

Q. And what is your MAIN reason for not wanting to provide your [ANSWER PREVIOUS QUESTION]

7.3 OMITTING INFORMATION FROM FORMS

A measure of sensitivity to privacy concerns is how often people omit details from forms. Information has been left off forms by 80% of Australians – and the proportion is increasing. Further, 28% always or often engage in this behaviour– up from 24% in 2004 and 22% in 2001.

Chart 7. Frequency with which information is omitted from forms



Q. When completing forms or applications that ask for personal details, such as your name, contact details, income, marital status etc, how often, if ever, would you say you leave some questions blank as a means of protecting your personal information?

Those more likely to leave information off forms:

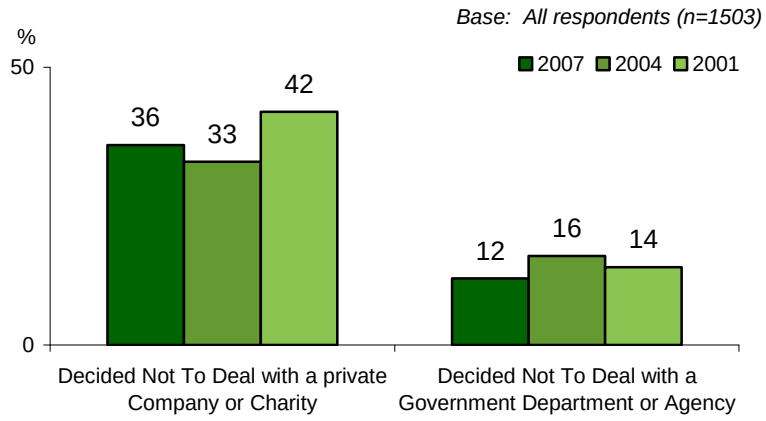
- live in metropolitan areas (82% cf. 78% of those living elsewhere)
- have a tertiary qualification (84% cf. 76% of those with Year 12 equivalent or less).
- live in Victoria (85%)

Retirees or those living in households earning less than $25,000 (70% and 75% respectively) were the least likely to leave information off forms.

7.4 AVOIDED DEALING WITH AN ORGANISATION TO PROTECT PERSONAL INFORMATION

Another measure of how concerned people are about privacy is whether or not they have decided against dealing with an organisation because of privacy concerns. The proportion who said they had decided not to deal with an organisation due to concerns about the handling of their personal information has not shown a great deal of fluctuation since 2001. As with previous surveys, respondents are more likely to have decided not to deal with a *business or charity* (36%) than *a Government department* (12%).

Chart 8. Decided NOT to deal with an organisation to protect personal information



Q. Firstly, have you ever decided not to deal with a private company or charity because of concerns over the protection or use of your personal information?
Q. Have you ever decided not to deal with a government department because of concerns over the protection or use of your personal information?

The proportion who avoided dealing with *a business or charity* (36%) was higher than in 2004 (33%), but still lower than that recorded in 2001 (42%). The proportion who had decided not to deal with *a government department or agency* at 12% was the lowest recorded to date. The proportion was 16% in 2004 and 14% in 2001.

Those more likely not to have dealt with a business or charity included:

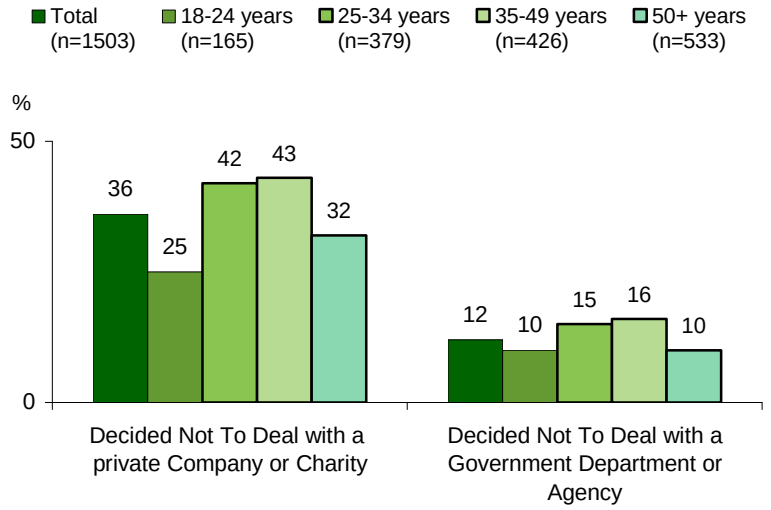
- Those living in metropolitan areas (43% cf. 39% elsewhere)
- Those with tertiary qualifications (43% cf. 39% Year 12)
- Upper white and upper blue collar workers (40%)

Overall, 14% of Australians had decided not to deal with *Government departments.* The only groups to vary significantly from the national average were those not working (19%) and retirees (8%).

As shown in Chart 9, middle aged Australians are more likely than other Australians to say they have not dealt with either type of organisation due to concerns about their personal information.

Chart 9. Decided NOT to deal with an organisation by age

Base: All respondents (n=1503)

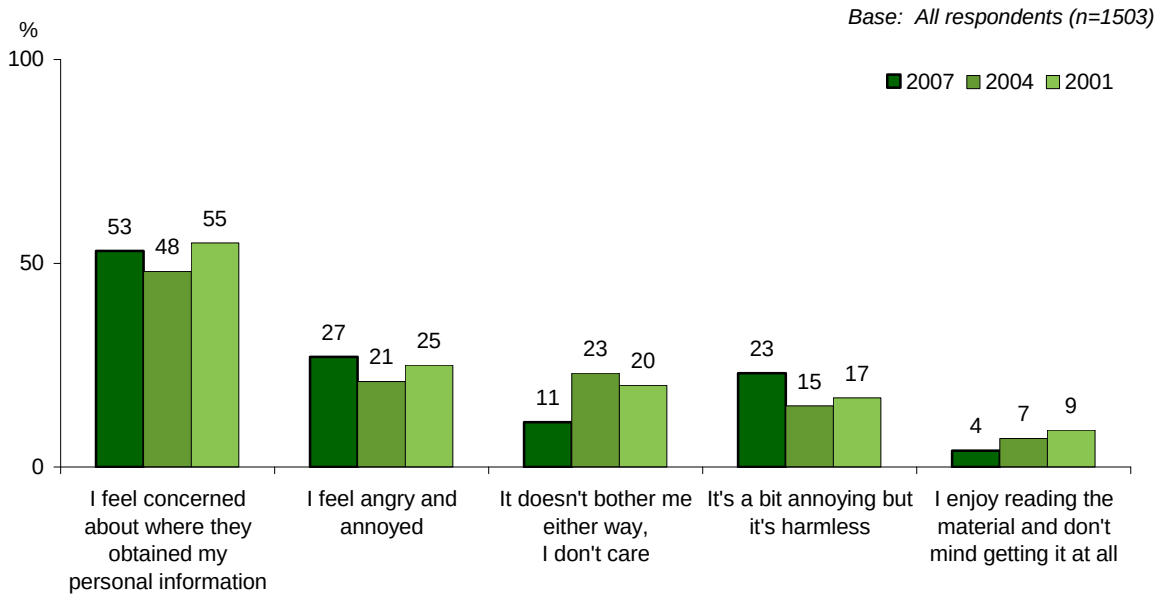


Q. Firstly, have you ever decided not to deal with a private company or charity because of concerns over the protection or use of your personal information?
Have you ever decided not to deal with a government department because of concerns over the protection or use of your personal information?

7.5 ATTITUDES TOWARDS UNSOLICITED MARKETING MATERIAL

Respondents were read five statements as shown in Chart 10 and asked to choose the one that describes how they feel when they receive unsolicited marketing material the best. Some respondents chose more than one option, as was the case when this question was asked in previous studies, therefore responses in Chart 10 add to more than 100.

Chart 10. Reactions to unsolicited marketing material



Q. Which of the following statements best describes how you generally feel when organisations that you have never dealt with before send you unsolicited marketing information?

The community's reactions are gradually becoming less favourable. Australians' main reaction is to be concerned about how direct marketing organisations obtain their details (53%). This was up from 2004 (43%), yet similar to 2001 (55%). There was an increase in the proportion feeling angry and annoyed when they receive unsolicited marketing material, up from 21% in 2004 to 27%.

Overall, the proportion showing annoyance or concern has remained stable at 80%. The proportion of Australians who were not bothered by such material has halved from 23% to 11%. The same shift has been seen over a longer time frame amongst those who enjoy receiving the material – only 4% currently enjoys it compared with 9% in 2001.

Age and employment status were the main discriminating factors underpinning attitudes:

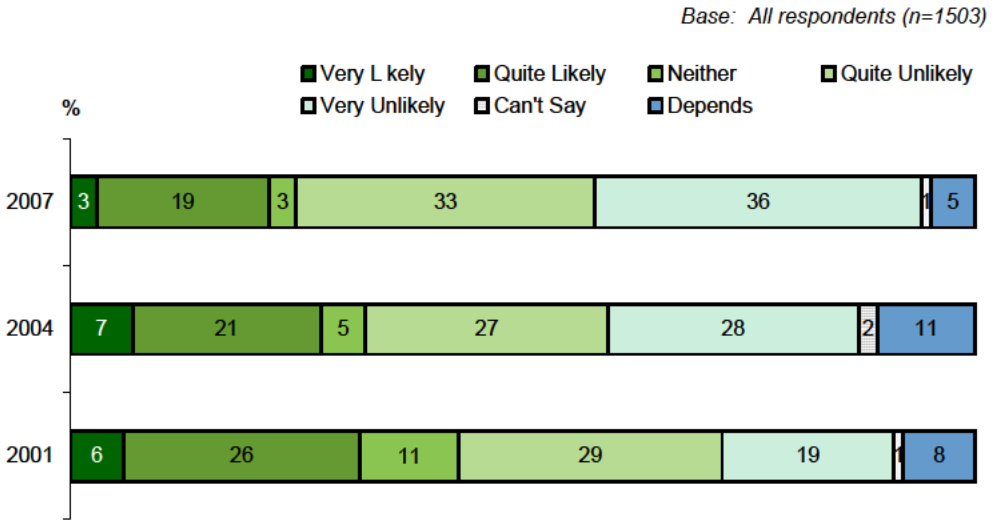
- Those aged 35-49 years (61%) were more likely than those aged 18-24 years (44%) to be *concerned about where organisations had obtained their personal information*.
- Those aged 18-24 (17%) were more likely than the national average to say *they don't care and are not bothered* by unsolicited marketing material.
- Employers or the self-employed (35%) are the most likely group to be *angry and annoyed* when they receive unsolicited marketing material.

7.6 ATTITUDES TOWARDS PROVIDING PERSONAL INFORMATION FOR BENEFITS

This section covers community attitudes towards providing personal information if they were offered a discount or the chance to win a prize.

As shown in Chart 11, there is clearly a declining trend in willingness to provide personal details in exchange for a discount. Furthermore, the proportion unsure of whether or not they would provide information has decreased since 2004.

Chart 11. Likelihood of providing personal information for discount



Q. Generally, how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive discounted purchases?

Twenty two percent (22%) would be likely to provide personal information to an organisation for discounted purchases. This compares to 28% in 2004.

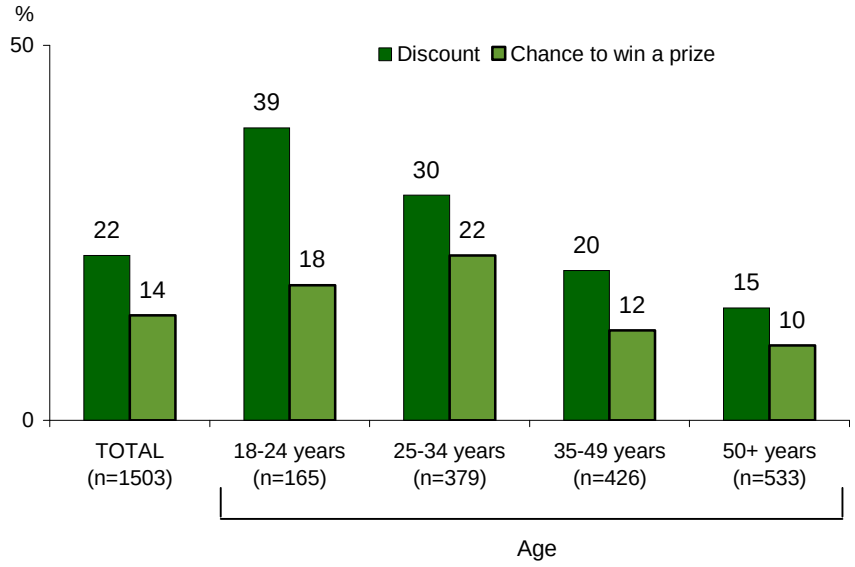
The profile of those likely to provide personal information in exchange for a discount remains the same as in past measures – it decreases with increasing age. However, even those most likely, the 18-24 year age group, are significantly less likely to do this now (39% compared with 54% in 2004).

The likelihood of providing personal information in exchange for a prize, at 14% of the population, is much lower than would give it for a discount (22%).

Younger age groups were again the most likely to say they would provide personal information to win a prize, (18-24 years – 18%, and 25-34 years – 22%). Only 10% of respondents over 50 years old would be likely to provide information if a prize was offered.

Chart 12. Proportion likely to provide personal information for discount or prize

Base: All respondents (n=1503)



Q. Generally, how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive discounted purchases?

Q. And how about if it meant you would have a chance to win a prize?

8.0 BUSINESSES AND PRIVACY

Business practices and community attitudes towards them are an important topic in privacy because businesses handle large volumes of personal information. Topics covered in this section are the:

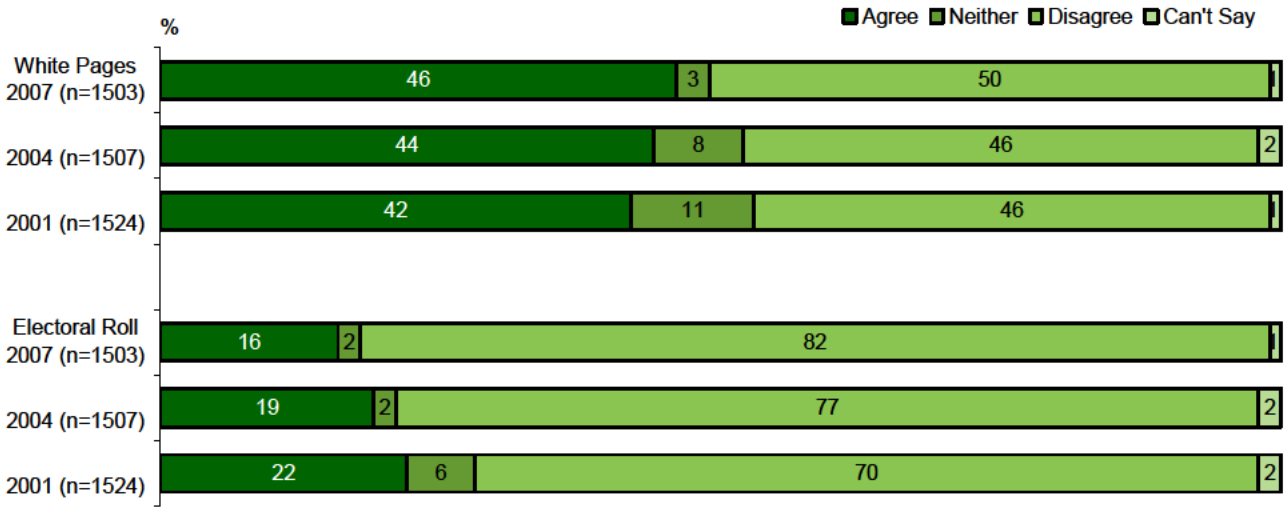
- use of public lists, such as the Electoral Roll and the White Pages telephone directory, for marketing purposes;
- degree to which the community regard certain scenarios as misuses of information; and
- levels of concern in the community regarding businesses sending personal information overseas for processing.

8.1 USE OF THE ELECTORAL ROLL AND WHITE PAGES FOR MARKETING PURPOSES

Australians were polarised as to whether businesses should be able to use the White Pages for marketing purposes. A slim majority disagrees (50%) and just under half (46%) agrees with this proposition – significantly more than agreed to use of the Electoral Roll as Chart 13 shows. Australians are increasingly against the practice of using the Electoral Roll for marketing purposes, with 82% saying they disagree with this practice, compared with 77% in 2004 and 70% in 2001.

Chart 13. Use of the Electoral Roll and White Pages for marketing purposes

Base: All respondents (n=1503)



Q. I would like you now to think about your privacy and businesses. I'm going to read you a number of statements and I'd like you to tell me whether you agree or disagree with each:
a) businesses should be able to use the electoral roll for marketing purposes
b) businesses *should be able to collect your information from the White Pages telephone directory without your knowledge for the purposes of marketing*

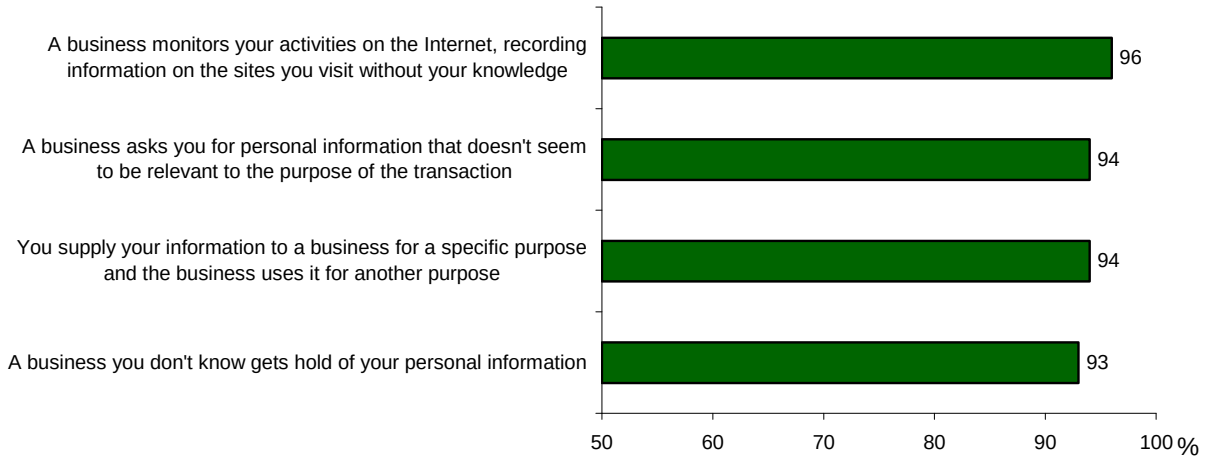
8.2 MISUSES OF PERSONAL INFORMATION BY BUSINESSES

Respondents were read four scenarios as shown in Chart 14 and asked whether or not they felt each was a misuse of personal information. The vast majority regarded all the scenarios as misuses of personal information, although they were slightly more likely to say that *monitoring activity on the Internet* (96%) was a misuse of information than the other scenarios (93-94%).

Younger Australians aged between 18 and 24 (99%) were unanimous in agreeing that businesses that use personal information for something other than was originally agreed was a misuse of personal information. They were also less likely than the national average to say *that a business they do not know getting hold of their personal information* is a misuse of that information, with 90% agreeing compared with 93% of Australians.

Chart 14. Scenarios regarded as misuses of personal information by businesses

Base: All respondents (n=1503)



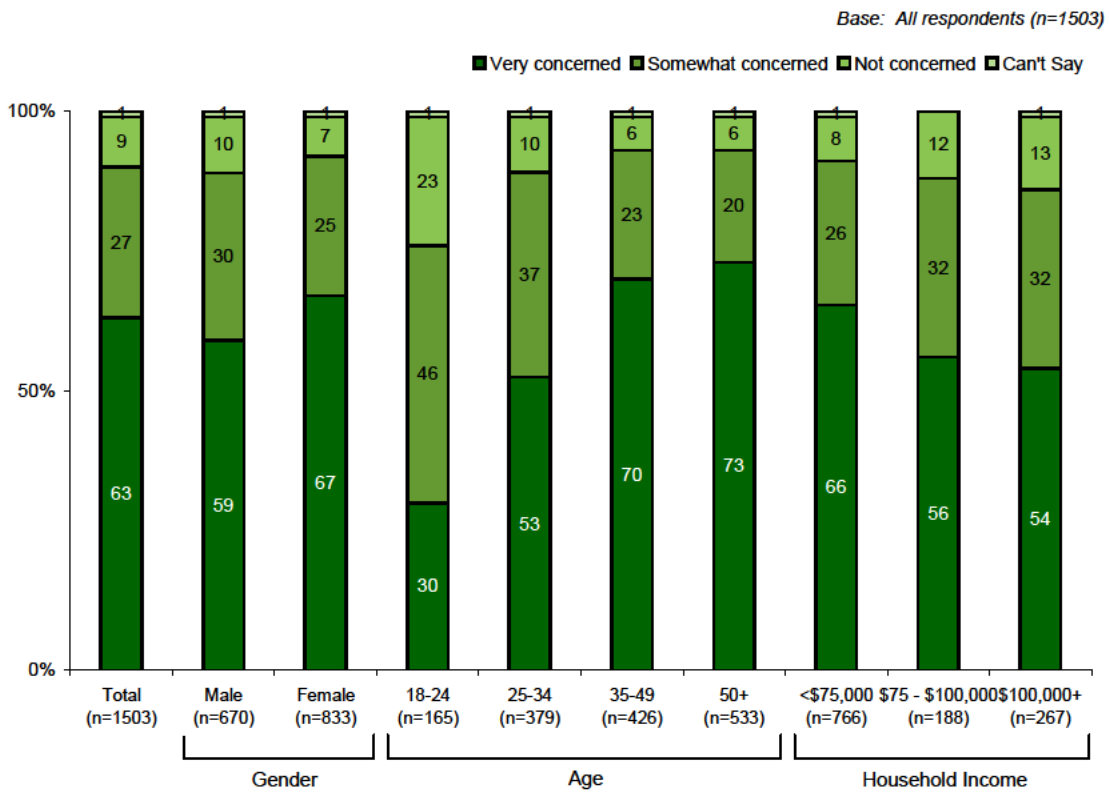
Q. Which of the following instances would you regard to be a misuse of your personal information?

8.3 LEVELS OF CONCERN ABOUT BUSINESS SENDING PERSONAL INFORMATION OVERSEAS FOR PROCESSING

The majority of Australians (90%) are concerned about their personal information being sent overseas, with 63% being *very concerned.* The level of concern varies amongst different groups. Those showing the highest level of concern being:

- Middle-aged Australians (35-49), with 70% saying they were very concerned. The proportion is similar (73%) for Australians aged over 50.
- People living in households earning under $75,000. Amongst these Australians, 66% are very concerned, compared with 54% of people living in households earning higher incomes.
- Females - with 67% being very concerned, compared with 59% of males.

Chart 15. Concern about business sending personal information overseas



Q. How concerned are you about Australian businesses sending their customers' personal information overseas to be processed?

Although not shown in the Chart, people working in lower blue collar occupations (76%) and people living in non-metropolitan areas (69%) also showed significantly higher concern levels.

9.0 GOVERNMENT DEPARTMENTS AND PRIVACY

There are many benefits of technology that could be utilised by Government departments and agencies to improve the efficiency and quality of the services they provide. In particular the ability to share information electronically means that once a client of one department updates their details, all departments they deal with could access the updated information and update their records automatically. This sections deals with community attitudes to facilitating and maintaining such services.

Specifically addressed are attitudes towards:

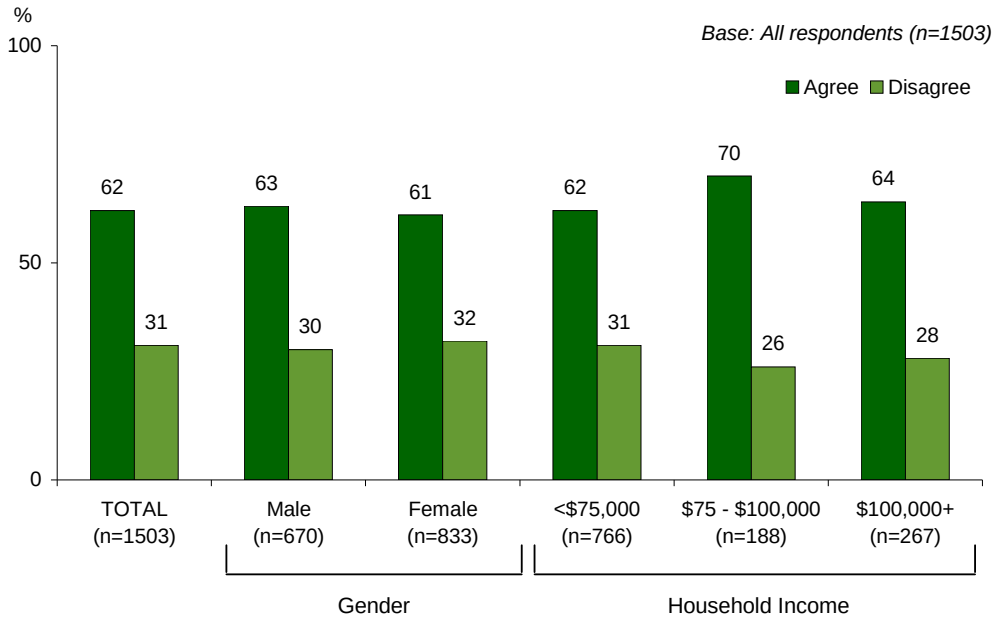
- a unique identifier for clients of all Australian Government departments;
- whether it is appropriate for Government departments to share information;
- the purposes for which Government departments should be able to share information; and
- what scenarios constitute misuses of personal information by Government departments.

9.1 ATTITUDES TOWARDS A UNIQUE IDENTIFIER FOR ALL AUSTRALIAN GOVERNMENT DEPARTMENTS

A unique identifier would allow Government departments to identify when they are dealing with the same person as another government department and allow better tracking of Government clients resulting in improved services and efficiency.

Support for a unique identifier has increased from 53% in 2004 to 62% in 2007. This increase is driven by those who *strongly agree* with the proposal (33% compared to 25% in 2004). The proportion who *partly agree* remains stable (29% cf. 28% in 2004).

Chart 16. Attitudes towards a unique identifier for all Australian Government departments



Q. If it was suggested that you be given a unique number to be used for identification by all Commonwealth Government departments and to use all Government services, would you be in favour of this?

As shown in Chart 16, the highest level of support overall came from respondents who live in households earning between $75,000 and $100,000 per annum (70%). Other respondents displaying above average support were those who:

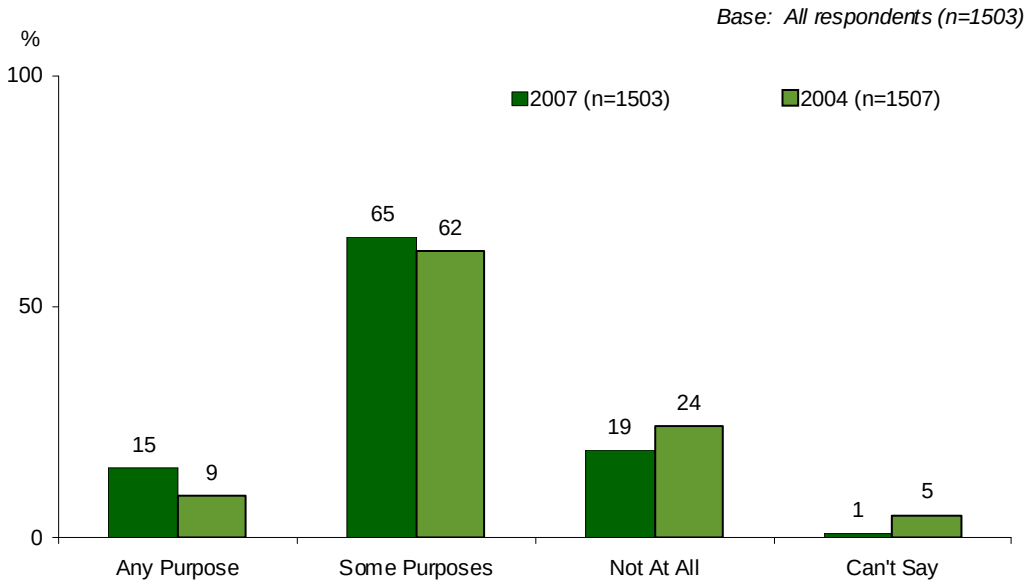
- Live in non-metropolitan areas (65%)
- Live in South Australia (67%).

Support was lower amongst those aged 18-24 years (54%) and Western Australians (52%).

9.1.1 Sharing of personal information between Government departments

The proportion of those who believe that Government departments should be able to cross-reference or share information about Australians remains significantly greater than those who do not think information should be shared. Further, the proportion in favour of sharing information has increased to 80% from 71% in 2004. Now 19% believes that information should be shared for *any purpose* (cf. 10% in 2004), with 65% continuing to say that information should be shared but only for *some purposes*.

Chart 17. Circumstances under which Government departments should be able to share information



Q. Do you believe Government departments should be able to cross-reference or share information in their databases about you and other Australians for any purpose, some purposes or not at all?

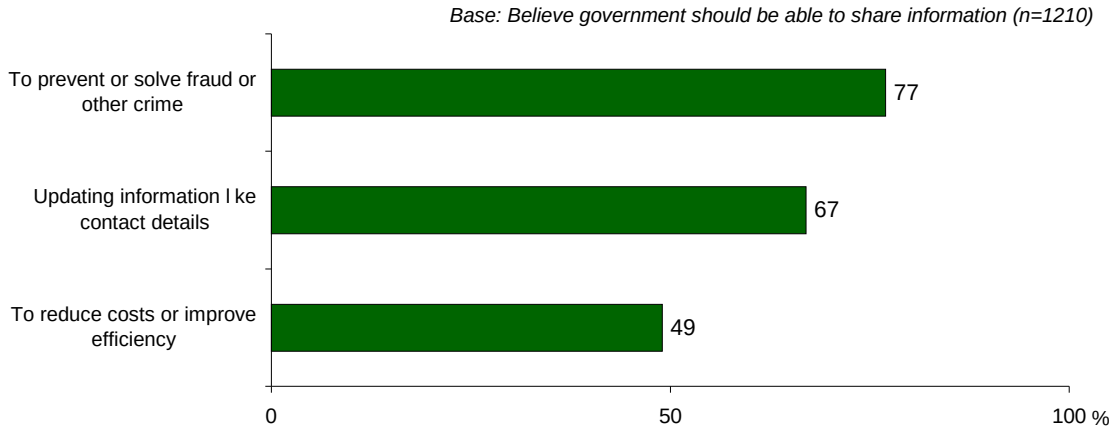
The results in 2007 echo those from 2004 with attitudes varying depending on gender, age and income. In particular:

- Males (17%) were more likely than females (13%) to say that Government departments should share information for *any purpose*.
- Agreement that *information should be shared for any purpose* increased with age and household income.

Respondents who were in favour of information being shared were asked to identify the circumstances in which this would be appropriate. Chart 18 shows that 77% believe it appropriate in the case of *crime prevention* and 67% support it for *updating contact details*.

Support for sharing information on the grounds of *reducing costs or increasing efficiency* is lower at 49%. Of those who said that Government departments should be able to share information, 20% did not agree to any of the purposes read out to them.

Chart 18. Purposes for which Government departments should be able to share information



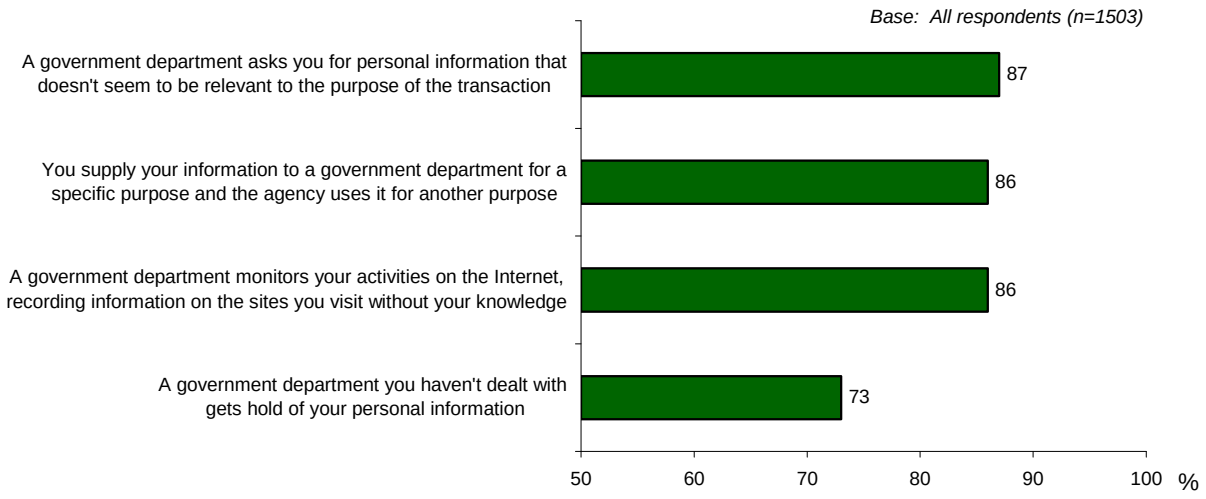
Q. For which of the following purposes do you believe Governments should be allowed to cross reference your personal information?

9.2 SCENARIOS REGARDED AS MISUSES OF PERSONAL INFORMATION BY GOVERNMENT DEPARTMENTS

Respondents were read four scenarios and asked to identify which ones they considered to be a misuse of their personal information. The majority thought that *asking for irrelevant information, using information for a purpose other than that for which it was provided* and *monitoring activities on the Internet* were equally misuses of their personal information (as shown in Chart 19). However, while 73% still believe that *a government department they had not dealt with getting hold of their personal information* constituted a misuse of that information, they were considerably less likely to regard this as a misuse compared with the other three scenarios.

Although the vast majority still regard most of these scenarios as misuses of their personal information, they are slightly less likely to think so than when the same scenarios are applied to businesses. In other words, Australians are more tolerant of government than of private businesses.

Chart 19. Scenarios regarded to be misuses of personal information



Q. Which of the following instances would you regard to be a misuse of your personal information?

These views were held consistently across the Australian public with the following exceptions:

- Females were more likely than males to believe the stated scenarios were misuses of information, with the exception of *monitoring activities on the Internet*, where both males and females were equally likely to feel it is a misuse of information.
- Those with an education up to Year 12 equivalent (80%) were more likely to believe that *a Government department they had not dealt with getting hold of their personal information* is a misuse of personal information.
- Tasmanians (97%) were the most likely to believe that *using information for a purpose other than that for which it was provided* was a misuse of personal information.

10.0 HEALTH SERVICES AND PRIVACY

This section examines community attitudes to privacy in the health system. Topics covered are attitudes towards:

- the inclusion of health information in a national health database, both generally and specifically in a de-identified form for research purposes;
- health professionals discussing and sharing patient information; and
- the disclosure of genetic information if a patient has an illness which a relative may also have.

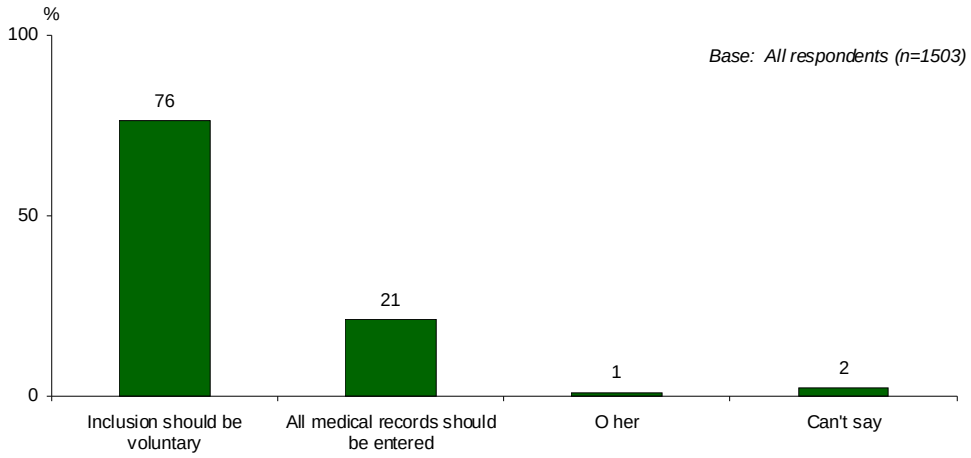
10.1 ATTITUDES TOWARDS INCLUSION IN A NATIONAL HEALTH DATABASE

A national health database would assist in improving the efficiency and quality of services provided by the healthcare system. Identifiable information could be used to access patients' medical histories if urgent treatment was required, as well as make it easier to transfer medical records between treating health professionals. De-identified information could be used by researchers to plan health services more accurately. Respondents were read the following introduction and then asked whether or not they thought inclusion in the database should be voluntary:

The idea of building a National Health Information Network has been put forward. If this existed it would be an Australia-wide database which would allow medical professionals anywhere in Australia to access a patient's medical information if it was needed to treat a patient. The information could also be used on a de-identified basis to compile statistics on the types of treatments being used, types of illnesses suffered and so on…

The majority (76%) of Australians believe that inclusion in the National Health Information Network should be voluntary. At 21%, the minority believes all medical records should be entered. A greater proportion (76%) believe inclusion should be voluntary (cf. 64% in 2004 and 66% in 2001). As in 2004, females (80%) were more likely than males (72%) to say this. Unlike 2004 however, there were no significant differences in attitudes between age groups.

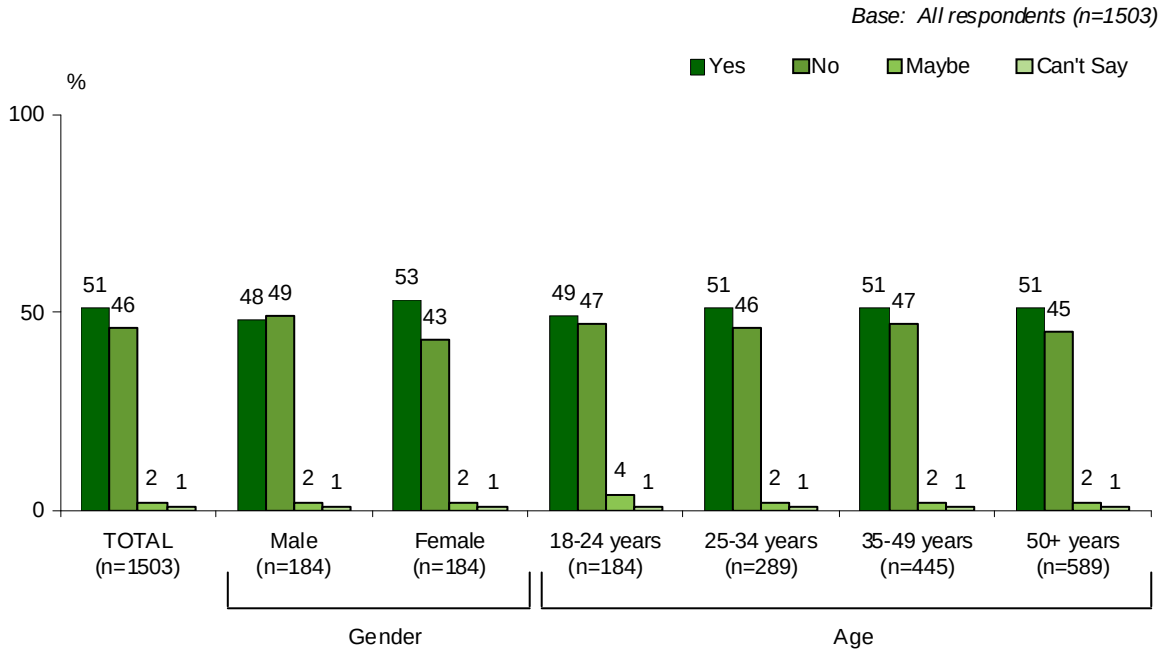
Chart 20. Inclusion of medical information in a National Health Information Network



Q. If such a database existed, do you think inclusion of your medical information should be VOLUNTARY, or should ALL MEDICAL RECORDS be entered without permission or consent?

Respondents were then asked whether, if such a database existed, permission should be sought before releasing their de-identified information. Females (53%) were more likely than males (43%) to say that permission should be sought.

Chart 21. Permission sought before de-identified health information released



Q. Health information is often sought for research purposes and is generally de-identified, that is, NOT linked with information that identifies an individual. Do you believe that an individual's permission should be sought before their de-identified health information is released for research purposes or not?

10.2 ATTITUDES TOWARDS HEALTH PROFESSIONALS SHARING PATIENT INFORMATION

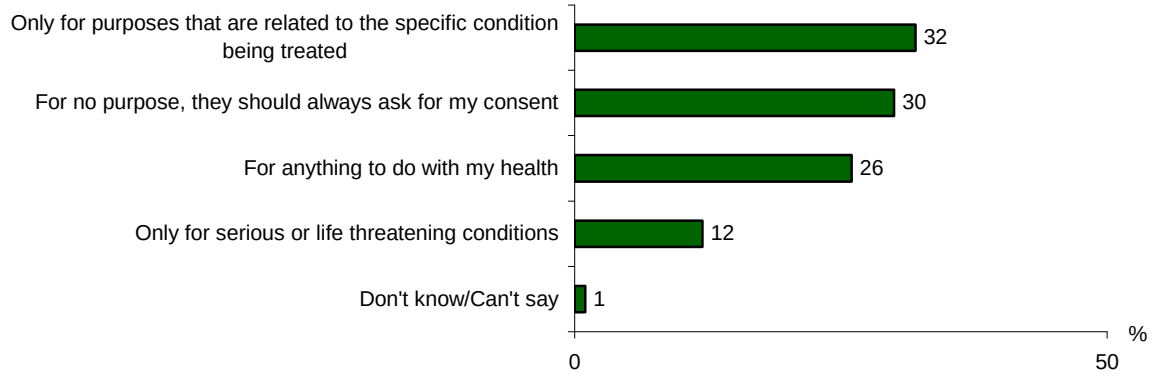
While opinions varied, 44% thought that health professionals should share health information, but only if *relevant to the condition being treated* (32%) or *if the condition was serious or life threatening* (12%). Thirty percent (30%) believed health professionals should share health information *only with the patient's consent. The proportion* believing *anything to do with a patient's health care* could be discussed between health professionals stands at 26%.

Attitudes to this proposition varied from state to state. Victorians (40%) were the most likely to believe that information should only be shared for the *purpose of treating a specific condition*. Western Australians (19%) were more likely than Victorians (10%) or those from NSW (11%) to say that information should only be shared *if the condition is serious or life threatening.*

Retirees (34%) were the most likely to support the sharing of information *for anything to do with my health care*.

Chart 22. Attitudes towards health professionals sharing information

Base: Respondents giving a single answer (n=1378)



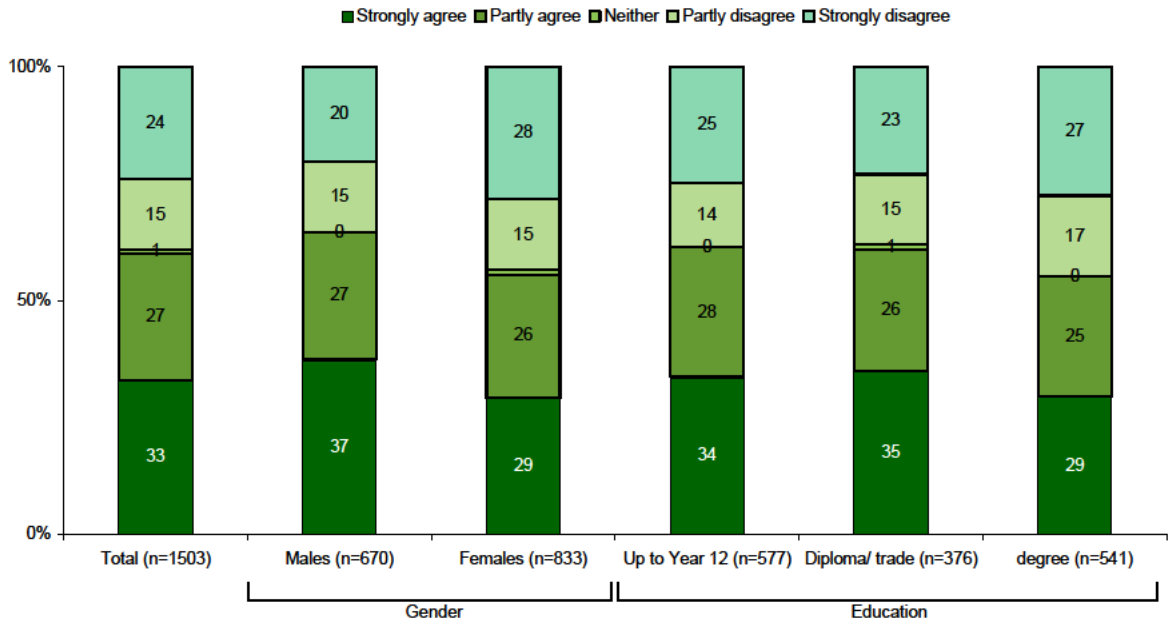
Some respondents provided multiple responses to this question. For analysis purposes, only the answers of respondents who gave a single response are shown.

Q. When do you think your doctor should be able to share your health information with other doctors or health service providers?

10.3 ATTITUDES TOWARDS DOCTORS DISCUSSING PERSONAL MEDICAL INFORMATION IN AN IDENTIFIABLE WAY

Respondents were asked whether they thought their doctor should be able to discuss their personal medical details with other health professionals in a way that identifies them without their consent. This was believed to be acceptable by 60% – the same proportion as in 2004 (60%) and a marked increase from 2001 (53%). Males (64%) were more likely than females (55%) to agree with this proposition. On the other hand those with a tertiary level education (54%) were less likely to agree than those educated up to Year 12 equivalent (63%) or with a diploma or trade qualification (61%).

Chart 23. Attitudes to doctors discussing patient details with other medical practitioners



Q. Do you agree or disagree that your doctor should be able to discuss your personal medical details with other health professionals – in a way that identifies you – without your consent if they believe this would assist your treatment?

10.4 ATTITUDES TO THE DISCLOSURE OF THE FACT THAT A PATIENT HAS A GENETIC ILLNESS - WITH AND WITHOUT CONSENT

Respondents were asked whether a relative of a patient with a genetic illness should be informed, and if so under which of the following circumstances:

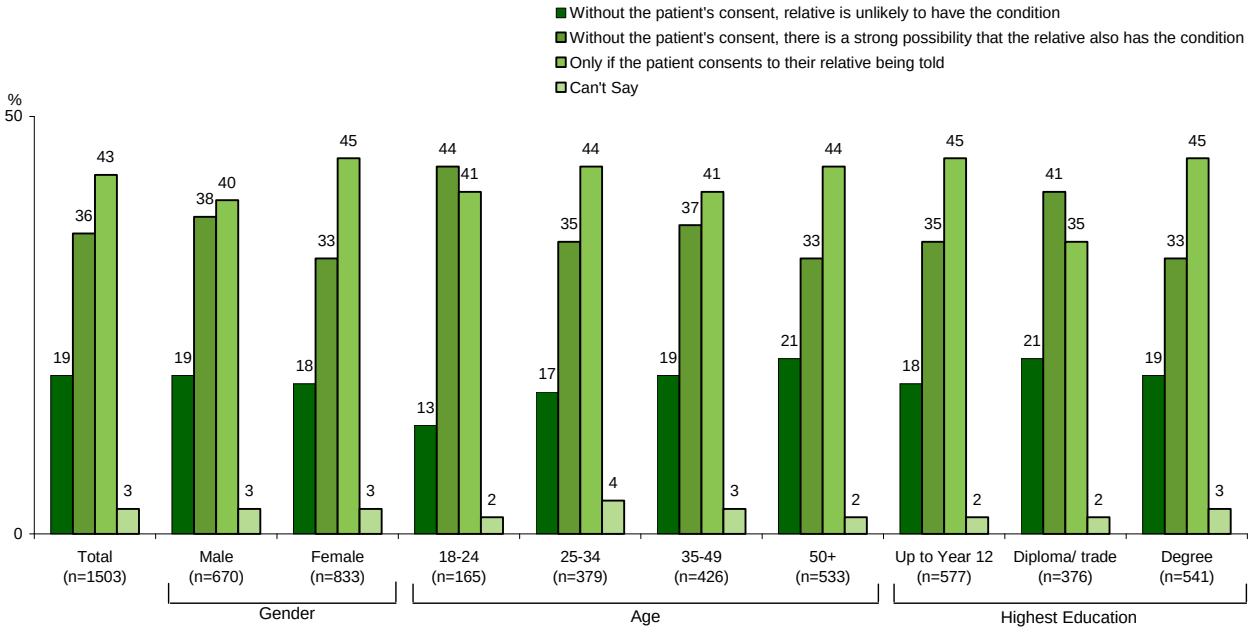
a) With the consent of the patient;
b) Without consent if there is a strong possibility that the relative has the condition; or
c) Without consent even if it is unlikely that the relative has the condition.

A slim majority (55%) believe that relatives should be told without the consent of the patient. This comprises 36% who believe that relatives should be told in the event that there is *a strong possibility they may have the illness* – especially Victorians (40%) and Australians aged under 24 (44%) – and 19% who are happy for the relative to be informed with *no consent even if it is unlikely that the relative has the condition.* Agreement with the latter statement increases with increasing age as Chart 24 demonstrates.

Forty three percent (43%) believe that relatives should be told only *with the consent of the patient.* Women are particularly likely to think this (45%).

Chart 24. Attitudes to the disclosure of the fact that a patient has a genetic illness - with and without consent

Base: All respondents (n=1503)



Q. If a person has a serious genetic illness, under what circumstances do you think it is appropriate for their doctor to tell a relative so the relative could be tested for the same illness?

11.0 PRIVACY IN THE WORKPLACE

As technology, such as computers, Global Positioning System (GPS) devices and recording equipment, become more prevalent in society, new privacy issues arise as employers can access more information about their employees. This section examines these issues as well as whether employees should have access to the information employers keep about them and the policies that govern how this information is kept.

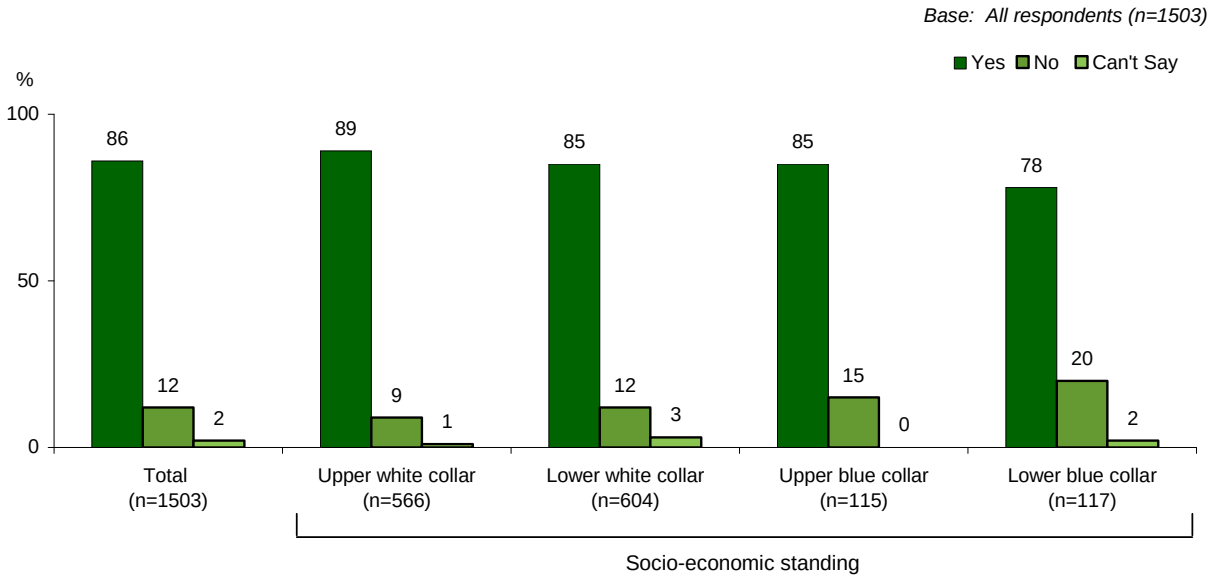
11.1 EMPLOYEES' ACCESS TO INFORMATION EMPLOYERS KEEP ABOUT THEM

Respondents were asked whether they thought employees should have access to information employers keep about them. As was the case when asked in 2004, 86% thought they should. However, unlike in 2004, there were no significant differences in the responses of people of different age and gender. Instead, those most likely to believe employees should have access to the information employers hold about them were:

- tertiary level qualified (91%) – in particular compared to those with up to a Year 12 education (82%);
- living in households with incomes over $100, 000 (90%); and
- those working in upper white collar occupations (89%).

As only 33 (2%) of the 1,503 respondents classified themselves as employers, the attitudes expressed here are predominantly those of employees (65%), retirees (19%), students (4%) and others not in the workforce (10%).

Chart 25. Attitudes towards employees having access to information their employer keeps about them



Q. Do you think employees should have access to the information their employer holds about them?

11.1.1 Employer activities and employee privacy

Respondents were asked to comment on whether and in what circumstances they believed it was reasonable for employers to:

- Read emails;
- Conduct drug and alcohol tests;
- Monitor vehicle locations where GPS is fitted;
- Monitor the workplace via surveillance equipment;
- Monitor the contents of employees' company computers; and
- Monitor telephone conversations.

Table 6. Attitudes towards employer activities and privacy

Employer Behaviour	Reading emails (n=1503) %	Drug & Alcohol Testing (n=1503) %	Monitoring Vehicle Locations (n=1503) %	Surveillance (n=1410)* %	Monitoring Everything on Computer (n=1423)* %	Monitoring Telephone Conversations (n=1355)* %
Whenever they choose	25	33	30	16	21	7
Only if they suspect wrongdoing	43	44	43	17	32	25
Not at all	30	20	25	22	28	29
For the safety and security of employees				44	18	
For training and quality control purposes						38

**Note: Some respondents provided multiple responses to this question. For analysis purposes, only the answers of respondents who gave a single response are shown.*

Q. I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing or not at all.

Australians are most likely to believe that employers should only read employees' emails, record what they enter into their computer, conduct drug and alcohol testing or monitor a vehicle location *if they suspect wrongdoing*. They are also most likely to believe that an employee should only be recorded on video or audio *for the safety and security of employees* and that the monitoring of telephone conversations should only occur for *training and quality control purposes*. Between 20% and 30% believe that employers have no right to undertake these activities under any circumstance.

There are differences of opinion:

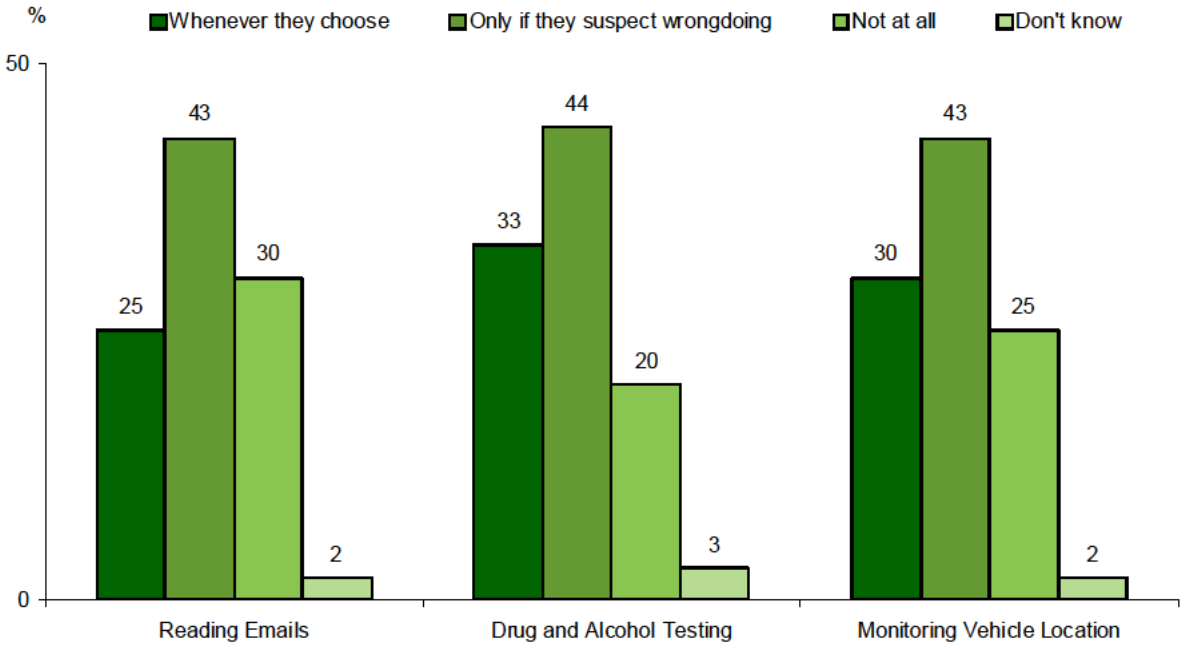
- Those working in white collar occupations are the most likely to believe that it is appropriate for employers to engage in these activities if they suspect wrongdoing.
- Those working in blue collar occupations and those living in non-metropolitan areas are more likely to believe that employers should be able to engage in such activities whenever they choose.
- Younger respondents, aged 18-34 years, are most likely to believe that employers should not engage in these activities at all.

11.2 ATTITUDES TOWARDS EMPLOYERS READING EMAILS, DRUG AND ALCOHOL TESTING AND MONITORING VEHICLE LOCATIONS

Respondents were asked to say whether they believed that employers were entitled to carry out three of the six activities, *whenever they choose*, *only if they suspect wrongdoing* or *not at all*.

Chart 26. Attitudes to employers reading emails, drug and alcohol testing and monitoring vehicle locations

Base: All respondents (n=1503)



Q. I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing or not at all.

In comparison with the 2004 survey, more respondents (43% cf. 38%) said that employers should read employee emails *only if they suspect wrongdoing* and less said that this is never appropriate (30% in 2007 and 34% in 2004) – part time employees in particular, are likely to hold this opinion (36%).

The wording of the response categories relating to random drug and alcohol testing was slightly different in this survey. The one category that remained the same, *whenever they choose* saw a significant increase, from 23% in 2004 to 33% in the current survey, suggesting there is more support for this practice now than in 2004. Although 44% believes

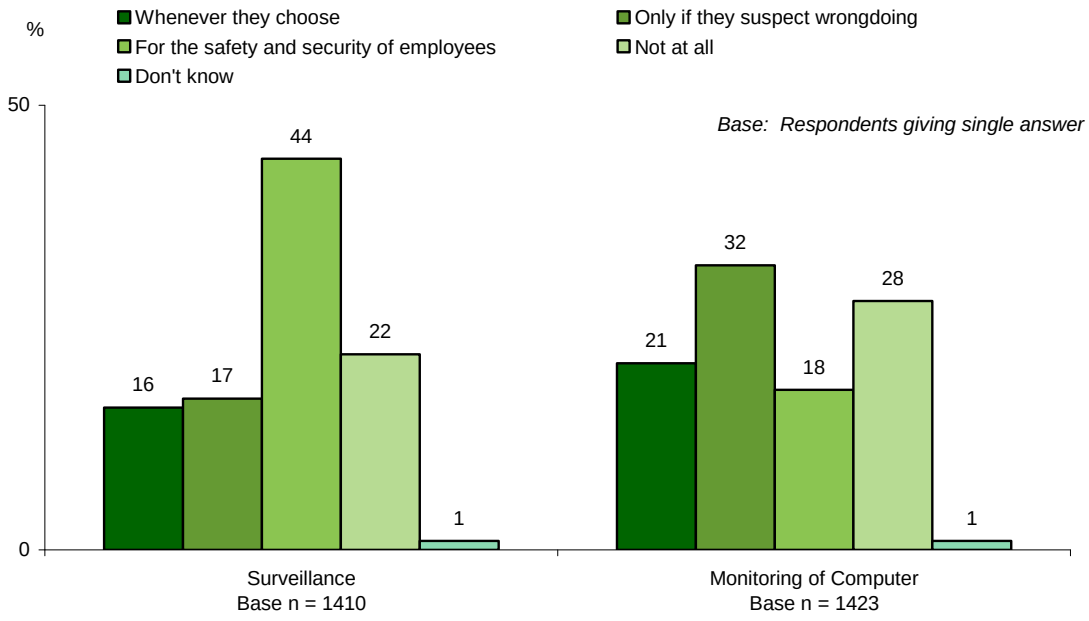
drug and alcohol testing should only happen if an employer suspects wrong doing, and 20% believes this should not happen at all – a significantly lower proportion than for the other two activities measured.

As GPS technology becomes more readily available, the question of whether it is appropriate to monitor employees' vehicle locations gains significance. Respondents were asked their attitudes to the monitoring of employees' work vehicles in the current survey. The most common response (43%) was that employers should only be able to do this if *they suspected wrongdoing*. The remainder was polarised between those believing employers could do this *whenever they choose* (30%) and those saying it should *not be done at all* (25%).

11.3 ATTITUDES TOWARDS EMPLOYERS USING SURVEILLANCE EQUIPMENT TO MONITOR THE WORKPLACE

Forty four percent (44%) of respondents felt it was reasonable for employers to use surveillance equipment in the workplace *for the safety and security of employees,* 19% said employers should only be able to use such equipment *if they suspected wrongdoing,* and 22% that employers should *not use it at all*. Only 16% thought that employers should be free to record their employees *whenever they choose.* Amongst young people aged 18 – 24, 24% approved of this behaviour in employers – higher than other age groups.

Chart 27. Attitudes towards employers using surveillance equipment and monitoring everything employees type into their computer.



Some respondents provided multiple responses to this question. For analysis purposes, only the answers of respondents who gave a single response are shown.

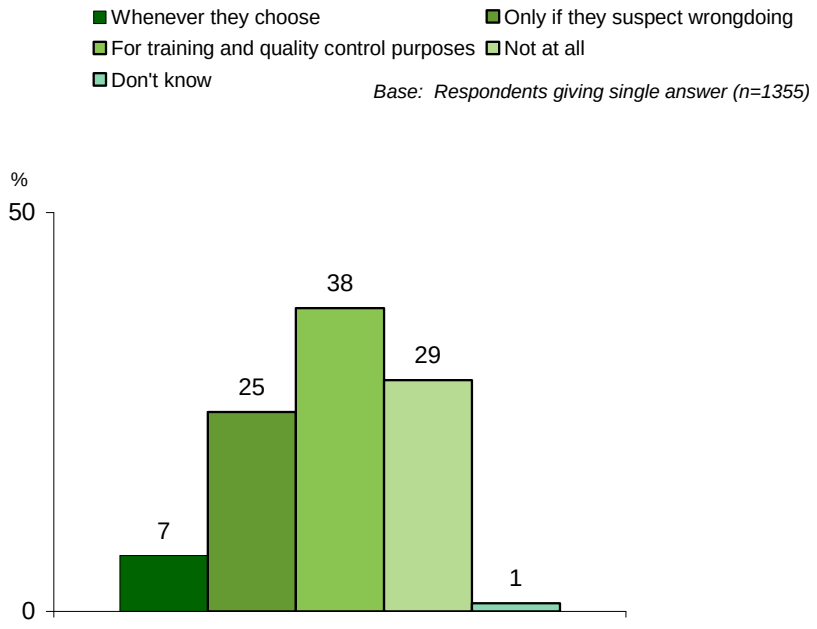
Q. I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing, for the safety and security of all employees, or not at all? (Note, these statements were read to respondents at the same time as 'monitoring employees' telephone conversations')

On the topic of when respondents think it appropriate for employers to monitor everything an employee types into their computer, views were more evenly spread - with 32% saying employers should only do this if they suspect wrongdoing and 28% thinking it unacceptable in any circumstances. The balance was divided between those who felt it was appropriate for safety and security only (18%), and those who had no misgivings about employers doing this whenever they choose (21%). In contrast to their attitudes on general surveillance, younger Australians were the least likely to think that employers should monitor the contents of computers whenever they choose (7%).

11.4 ATTITUDES TOWARDS EMPLOYERS MONITORING TELEPHONE CONVERSATIONS

Respondents were finally asked when they think it is appropriate for employers to monitor telephone conversations. As many organisations monitor frontline and call centre staff as standard practice, respondents had an extra category to choose from when answering this question, namely *for training and quality control purposes* – which was the most commonly selected response at 38%. This practice was believed by 25% to be appropriate from employers *only if they suspect wrongdoing* however a slightly higher proportion (29%) said *not at all.* Only 7% of respondents felt this activity was acceptable from employers *whenever they choose*.

Chart 28. Attitudes towards employers monitoring employees' telephone conversations



Some respondents provided multiple responses to this question. For analysis purposes, only the answers of respondents who gave a single response are shown.

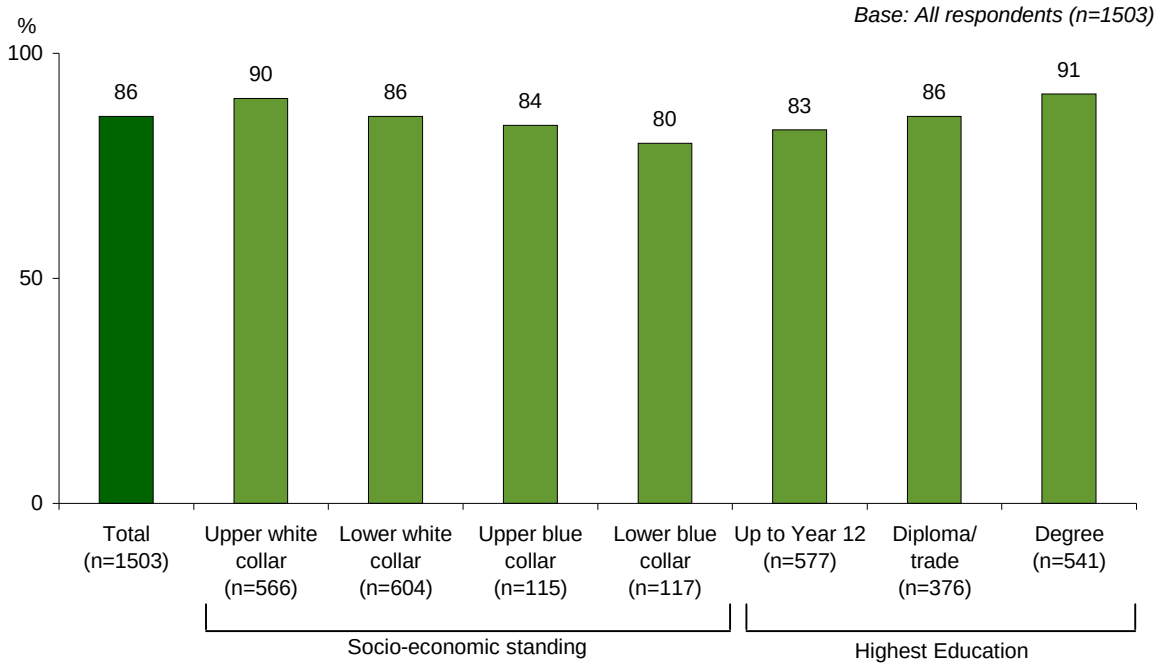
Q. I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing, for the safety and security of all employees, or not at all ? (Note, this statement was read to respondents at the same time as 'surveillance' and 'monitoring of computer')

11.5 IMPORTANCE OF EMPLOYER PRIVACY POLICIES

Respondents were asked how important they thought it was that employers had privacy policies that covered areas such as when employers would read work emails, randomly drug test employees, use surveillance equipment to monitor employees and monitor telephone conversations. In 2007, 86% thought privacy policies were important, slightly more than in 2004 (83%).

Respondents working in upper white collar occupations (90%) and those with a tertiary education (91%) were the groups most likely to think that employer privacy policies are important.

Chart 29. Importance of employer privacy policies



Q. How important is it to you that an employer has a privacy policy that covers when they will read employee emails, randomly drug test employees, use surveillance equipment to monitor employees and monitor telephone conversations

12.0 PRIVACY AND THE INTERNET

In March 2007 there were 5.7 million household Internet subscribers and 761,000 business subscribers[4]. Internet usage is clearly widespread in the community. The ease of intercepting and duplicating information in digital format makes the Internet a medium of high potential risk for the exposure of personal information.

This section examines community attitudes regarding the provision of personal information in electronic format versus more traditional formats such as hard copy and telephone as well as people's likelihood to provide false information as a means of protecting their personal information. Attitudes towards privacy policies on websites are also considered.

[4] *Internet Activity Survey*. March 2007. ABS Catalogue number 8153.0

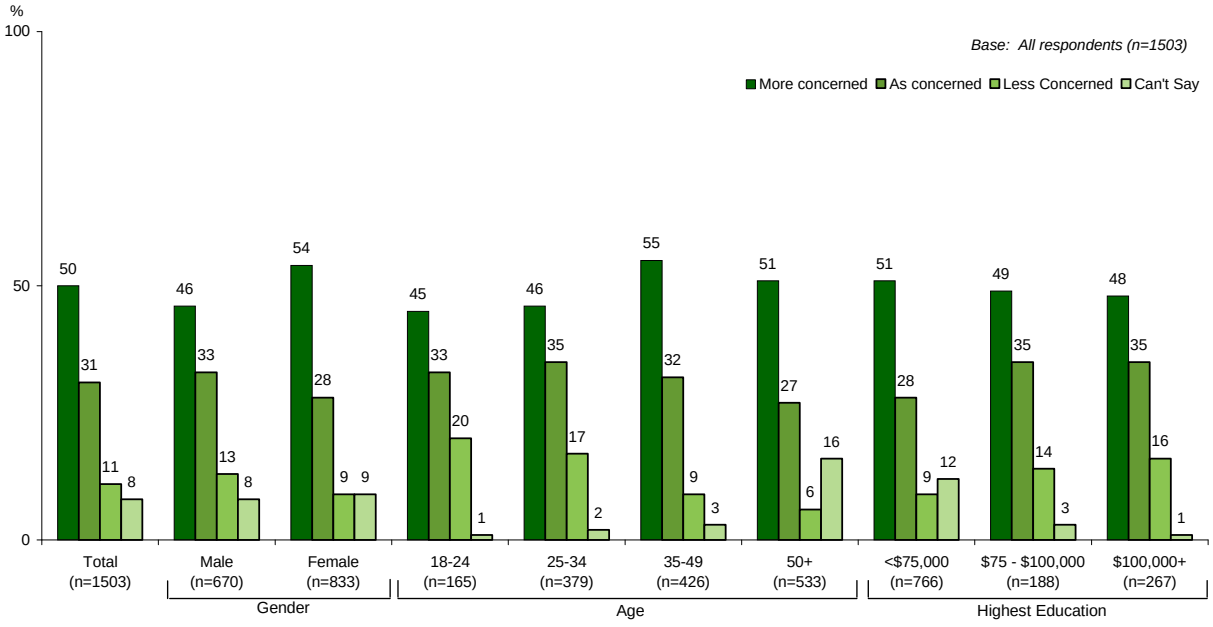
12.1 LEVELS OF CONCERN ABOUT PERSONAL INFORMATION ON THE INTERNET

Respondents were asked to state their level of concern about providing information over the Internet:

- in general compared with two years prior;
- compared with providing hard copy information; and
- compared with providing information over the telephone.

Half (50%) were *more concerned* about providing information over the Internet than they were two years ago, with 31% *as concerned* and 11% *less concerned*. A higher proportion of younger Australians aged under 24 claimed to be *less concerned* than two years ago. However four times as many young Australians claimed to be *more* or *as concerned* than they were two years ago.

Chart 30. Levels of concern about personal information on the Internet compared with two years ago

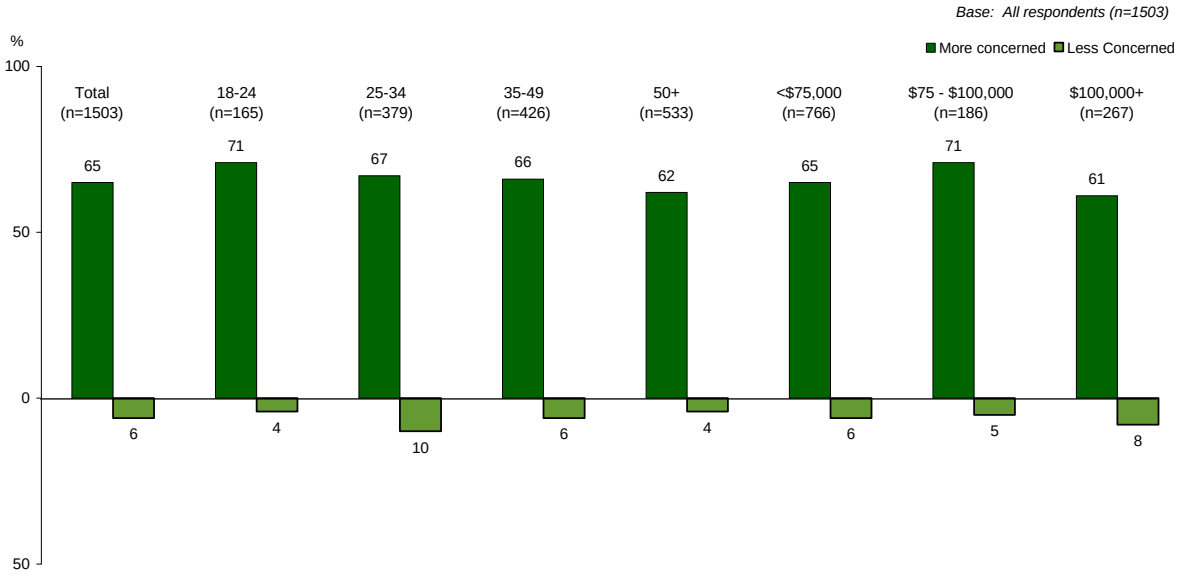


Q. Are you MORE OR LESS concerned about the privacy of your personal information while using the Internet than you were two years ago?

Reference to Charts 31 and 32 show that 65% of Australians feel *more concerned* about providing details online versus in hard copy format. The proportion feeling *more concerned* about providing details online versus over the telephone is lower at 45%. Conversely, only 6% of Australians feel *less concerned* using the Internet versus hard copy and one in eight

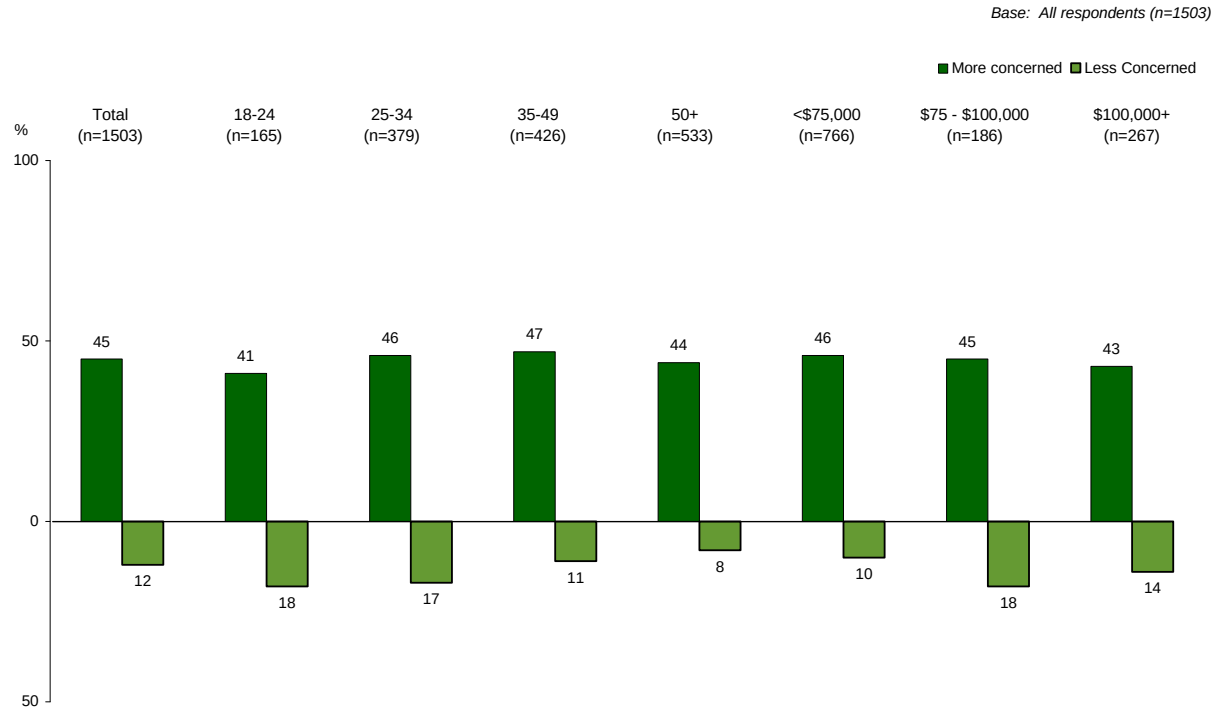
(12%) feels less concerned using the Internet as opposed to the telephone. The conclusion that can be drawn is that Australians believe the Internet is not as secure as other more traditional means of providing information. These charts also show that a great deal of similarity exists in responses across age and income with the exception that people living in households earning over $75,000 seem to be slightly less daunted by giving information over the Internet than others.

Chart 31. Concern about providing personal information over the Internet versus in hard copy



Q. Are you more or less concerned about providing your personal details electronically or online compared to in a hard copy/paper based format?

Chart 32. Concern about providing personal information over the Internet versus over the telephone



Q. And are you more or less concerned about providing your personal details electronically or online as opposed to over the telephone?

12.2 PROVIDING FALSE INFORMATION ONLINE AS A MEANS OF PROTECTING PRIVACY

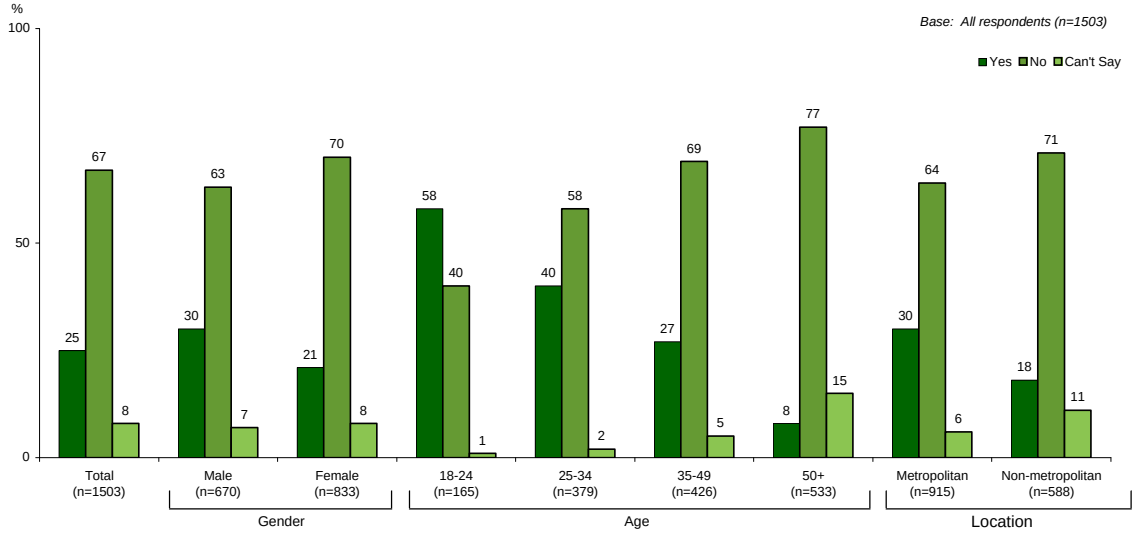
Respondents were also asked how often they provide false information on forms and applications as a means of protecting their privacy. Most saw no need to do this (67%) and said they did not provide false information, however 25% did feel a need to protect themselves in this way.

The propensity to provide false information fell dramatically with increasing age, with 58% of Australians aged 18-24 years having provided false information, compared with 8% of those aged over 50.

Other groups who felt more need to provide false information were those:

- living in households earning over $100,000 (34%);
- living in metropolitan areas (33%);
- who are tertiary educated (30%); and
- males (30%).

Chart 33. Providing false information in online forms



Q. When completing online forms or applications that ask for personal details, have you ever PROVIDED FALSE INFORMATION as a means of protecting your privacy?

12.3 USE AND IMPACT OF PRIVACY POLICES ON ATTITUDES TO WEBSITES

When asked whether they read privacy policies on websites, 33% said that they normally do. Respondents aged 25-34 (39%) were the most likely to do so, and females (36%) were more likely than males (30%) to read them.

Respondents who read privacy policies were asked what impact seeing the privacy policy had on their attitude to the website. The two most common responses were:

- *it helps me decide whether or not to use the site (27%);* and
- *it makes me feel more confident and secure about using the site (25%).*

13.0 IDENTITY FRAUD

A range of organisations have listed identity fraud and theft as both a growing concern to the Australian public and a growing problem[5]. This study endorses this point of view with Australians being almost unanimous (96%) in saying that ID fraud or theft is an invasion of privacy.

Currently published crime statistics do not provide time series data or a baseline on the incidence of its occurrence. In recognition of this, the Australian Bureau of Statistics is introducing a survey of Personal Fraud victimisation as an adjunct to its regular Crime Victimisation Survey collections. The pilot for this study was conducted in February-March of 2007 and the results of the survey, which is in field at time of writing (July to December, 2007) will be available in 2008.

As this is a relatively new area of investigation, respondents were read the following introductory statement before being asked questions on the subject

I'm now going to ask you a few questions about providing photo identification and identity fraud and theft. By identity fraud and theft I mean where an individual obtains your personal information (eg. credit card, drivers licence, passport or other personal identification documents) and uses these to fraudulently obtain a benefit or service for themselves.

[5] eg 'When bad things happen to your good name' - Australasian Centre for Policing Research; 'id Theft – A kit to prevent and respond to identity theft' The National Crime Prevention Program (in association with others) – Towards a Safer Australia.

13.1 INCIDENCE OF ID FRAUD AND THEFT

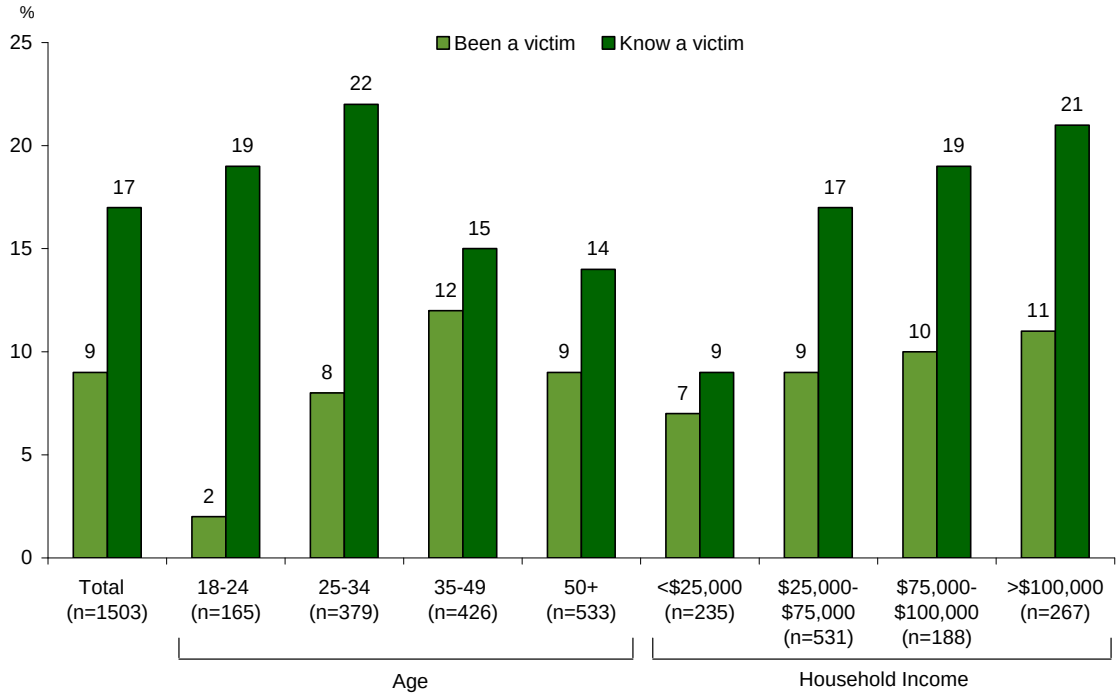
Respondents were asked whether they or someone they know has been the victim of ID fraud or theft. Overall 9% of Australians claimed they had been the victim themselves and 17% knew someone who had been the victim.

Generally speaking, the likelihood of being a victim is highest amongst people working in upper white collar professions, amongst those aged between 25 and 49, and amongst Western Australians. The characteristics of those who know someone who has been the victim are less well defined as a broader snapshot of the community fits into this category.

More details are shown in Chart 34 which identified the following factors are being influential in underpinning Australians' likelihood of being a victim or knowing someone personally who has been:

- Age – people aged 35 – 49 are the group most at risk themselves (12%) and to know someone who has been the victim (22%), with those aged under 24 (2%) being the least likely to have been a victim, but quite likely to know someone who has been (19%).
- Location – Western Australians reported a significantly higher incidence of being the victim of ID fraud and theft (14%).
- Employment – people who are employed (especially if full-time) are more likely to know someone that has been the victim of this type of crime (18%).
- Household income – the likelihood of knowing someone who have been the victim of ID fraud or theft increases with increasing household income (to 21% of people living in households earning more than $100,000).

Chart 34. Incidence of being the victim or personally knowing a victim of ID fraud/theft



Q. Have you or someone you personally know ever been the victim of identity fraud or theft?

The majority of Australians are concerned about becoming a victim of identify fraud or theft, with 60% saying they are *concerned*, and 17% of this total saying they are *very concerned*. Not surprisingly, the profile of those displaying the highest levels of concern matches the profile of those who have been victims, while those displaying the least concern do not coincide with those showing high concern levels. Western Australians hold polarised views on this issue with citizens either being more likely to be *very concerned* or *not concerned at all*.

People living in middle income households ($25 – $100,000) are the most concerned. Those earning less or more still show signs of concern but at reduced levels.

13.2 ACTIVITIES THAT MOST EASILY ALLOW IDENTITY FRAUD OR THEFT TO OCCUR

The Australian Federal Police and the Attorney-General's Department, amongst others, have produced consumer guides aimed at reducing or eliminating identity fraud and theft. These guides suggest the two key ways in which an identity may be stolen are:

- Physical loss or theft of personal documentation (wallet, credit and other ID); and
- Interception of mail containing personal information – both electronic and physical.

Respondents were asked for their views.

Table 7. Respondents' views on ways in which identity fraud and theft can occur most easily

Activities that allow ID theft to occur	Total (n=1,503) %
Using the internet in general	27
Buying items online	11
Online Banking	11
Nett mentions of Internet/online*	**45**
Losing/having ID, wallet, passport and other documentation stolen	22
Using credit card/losing sight of card	20
Giving out too much personal information to organisations and businesses	19
Having documentation stolen from mailbox or bin	14
Using ATMS/teller machines/EFTPOS	7
Buying items over the phone	3
Other	4
Don't know	4

Base: all respondents
** This is a multiple response question. The nett figure shown is the proportion of all respondents who mentioned one of more of the three categories above it.*

Q. What activities do you think most easily allow identity fraud or theft to occur?

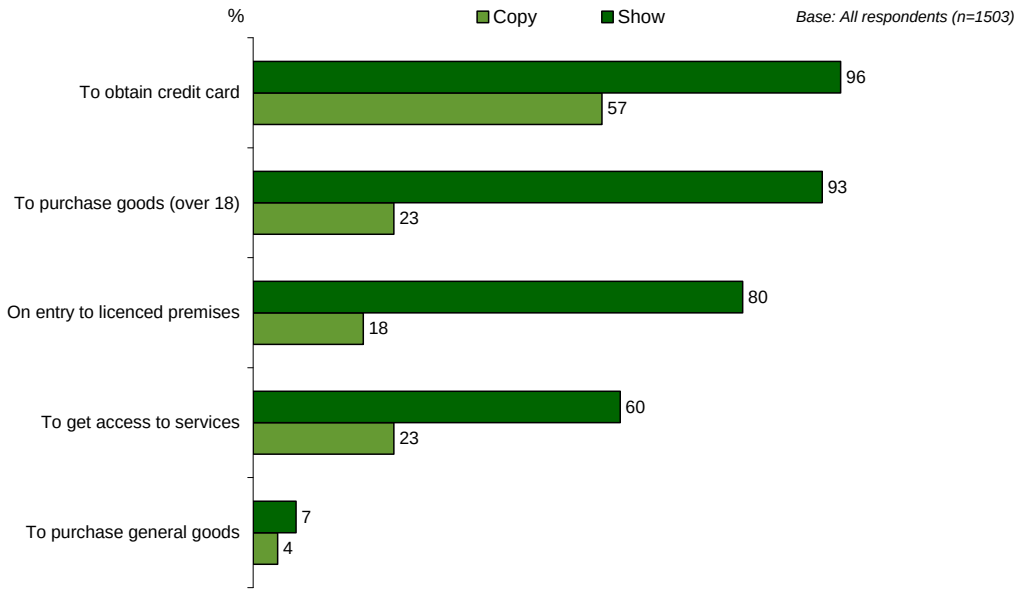
In aggregate, concerns about the possibility of identity fraud and theft over the Internet increase with increasing income. Amongst people living in households earning over $100,000, 52% nominated one or more ways that identity fraud of theft could occur via this medium.

Given they were the most likely to report being the victims of identity fraud and theft, it is interesting to note that Western Australians were significantly more likely than others to offer a *don't know* response to this question (7%). Concern about using credit cards increases with age as does concern over online banking, to the point where people aged over 50 have significantly different views to those aged under 25.

13.3 SHOWING AND COPYING IDENTIFICATION DOCUMENTS

Respondents were asked whether they considered it was reasonable either to show identification documents or to have a copy of those documents made in a range of situations. Their responses are shown in Chart 35.

Chart 35. Acceptability of having to show identification documents or have them copied



Q. Do you think it is acceptable that you need to show / copy identification documents (such as a drivers license or passport) in the following situations:

In all cases, the proportion believing that it is acceptable for copies of documents to be made is significantly lower than agrees it is acceptable for them to be shown.

The requirement to show identification documents to purchase everyday goods, clearly, would not be acceptable to the majority of Australians. However, the majority supports showing documentation for the other ideas put to them.

Support for showing identification documents on entry to a licensed premises and for purchasing goods that require the purchaser to be an adult declines with increasing age. Support levels are otherwise very similar across the country and respondents of all types.

The majority only support making a copy of identification documents for credit card applications. Otherwise acceptance levels are below a quarter of the population and similar across all types of respondent.

Support for copying documents is only acceptable to the majority for obtaining credit cards. For this activity 57% of Australians agrees that copying identification documentation is acceptable. Support drops dramatically with only 23% supporting copying documentation to purchase goods *that requires the purchaser to be over 18*, or *get access to services.* Support falls further to 18% to *gain entry to licensed premises* and only 4% support having documents copied to *purchase general goods*.

14.0 PRIVACY IN PUBLIC PLACES – CCTV

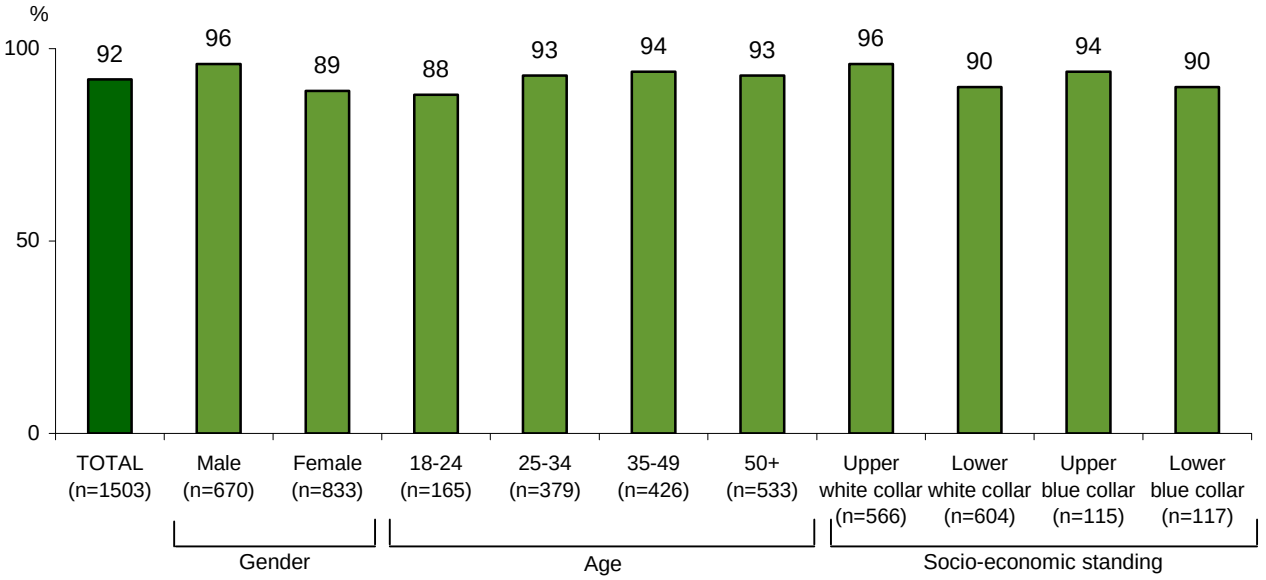
Most Australians (92%) are aware of closed-circuit television (CCTV). Given their greater likelihood to be in places with CCTV installed (pubs, nightclubs, restaurants, bars and throughout the public transport system) it is interesting that 88% of Australians aged under 24 are aware. The fact that many of this group had not completed Year 12 and/or earn under $25,000 suggests that at least some of them may still be high school students.

14.1 AWARENESS AND CONCERNS ABOUT CCTV

Awareness of CCTV increases with increasing household income, education and socio-economic standing.

Chart 36. Awareness of CCTV

Base: All respondents (n=1503)



Q Are you aware of or have you seen CCTV cameras?

Amongst those aware of CCTV cameras, 79% are not concerned about their use in public places. Concern lessens with increasing age. Victorians show higher levels of concern than other Australians. Although 80% of Victorians say they are *not concerned*, 16% are *somewhat concerned* – higher than across the rest of Australia. The proportion of people who are *very concerned* is stable across the country at less than 5%.

Given the generally low levels of concern, only 203 respondents in total were asked to enunciate their main concerns. These are shown in Table 8 and cannot be analysed in any more depth owing to the small number of respondents in segments such as state and even age. There are sufficient men and women answering this question to compare their responses. Reference to the Table shows that men are much more concerned that taped footage may be misused than women, otherwise their concerns are similar.

Table 8. Concerns about CCTV

CCTV concerns	Total (n=203) %	Men (n=117) %	Women (n=87) %
Information may be misused	54	60	45
Invasion of privacy	45	42	49
It makes me uncomfortable	13	13	13
Not effective in stopping crime/false sense of security	4	3	5
Other	4	4	4
Don't know	2	2	3

Base: concerned about CCTV (n=203)

Note that respondents were asked for one answer, but some gave more than one – therefore percentages do not add to 100.

Q. What is your main concern?

14.2 ACCESS TO CCTV FOOTAGE

Respondents were asked which organisations should have access to CCTV footage. Even those with concerns about CCTV, offered suggestions for appropriate use. On average, respondents were able to suggest 1.74[6] organisations each that they believed should have access. Responses were similar amongst Australians from all walks of life.

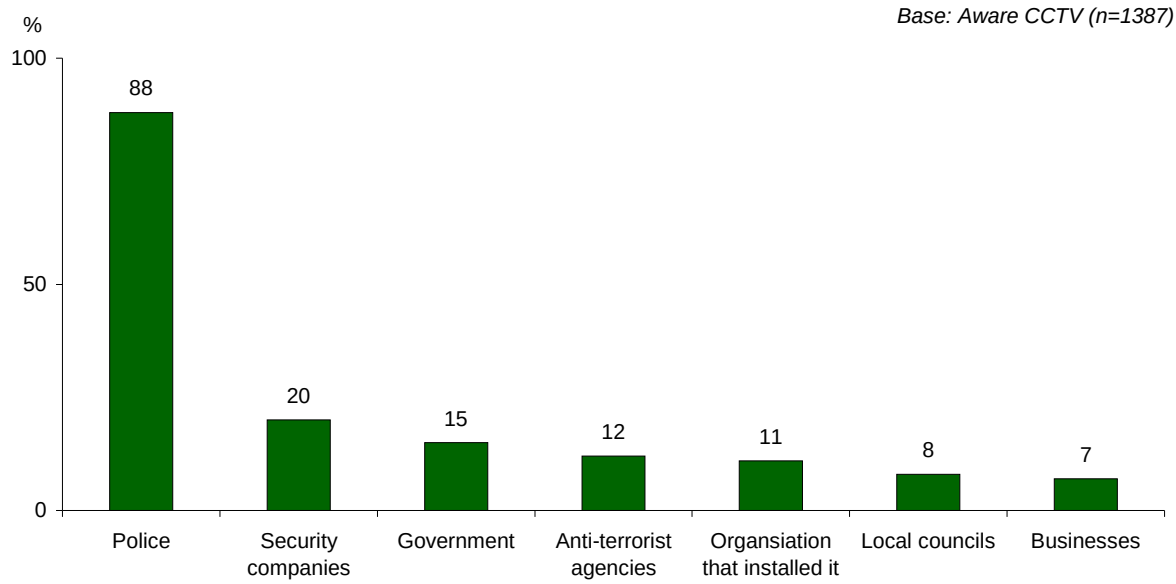
The organisation mentioned most that should have access was *the police* (88%), with support increasing significantly amongst Australians aged 25 and over. Whereas 75% of 19 – 24 year olds nominated *the police*, 86% of 25 – 35 year olds, rising to 91% of Australians aged over 50, nominated *the police*. Otherwise levels of agreement that the police should have access were consistent across respondents of all types.

Support for other organisations accessing footage was considerably lower. Security companies were nominated by 20%. Once again, support levels were similar across most types of Australians, with several notable exceptions – people who are not working are significantly more likely to nominate these organisations (26%), as are sales people and skilled workers (25% and 30% respectively). Chart 37 shows that 15% nominated the government, 13% anti-terrorist agencies and 11% nominated the company that installed the camera.

Although only 61 students were interviewed, they had significantly different views from other Australians in that they are less likely to nominate *the police* as an organisation that should access CCTV footage (76%) and more likely to say that government (28%), anti-terrorism law enforcement agencies (12%) and everyone (6%) should have access.

[6] This is the average number of responses each respondent gave to the question.

Chart 37. Organisations that should have access to CCTV footage



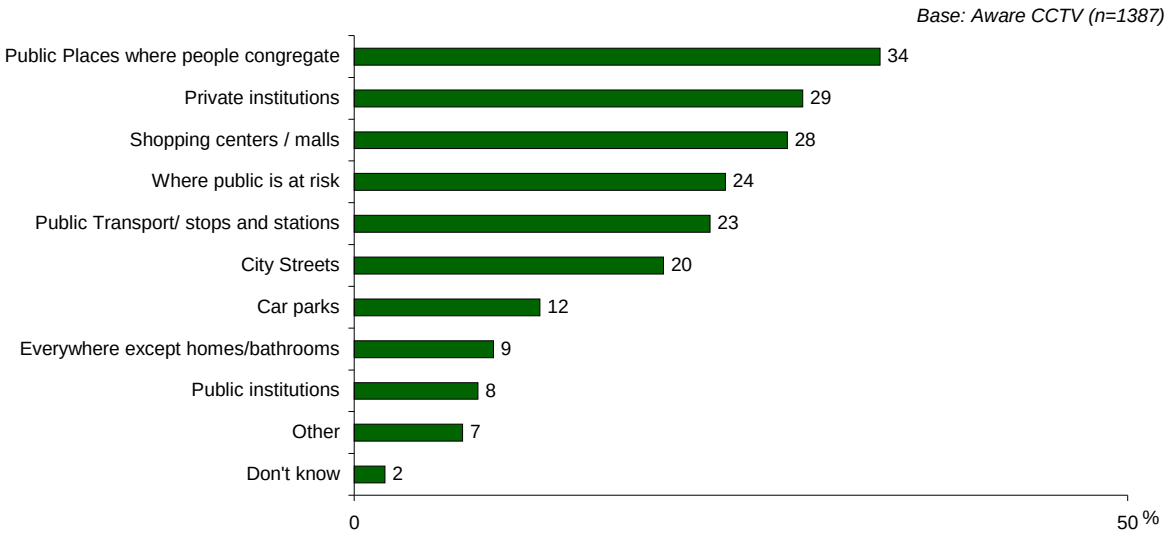
Note responses of less than 5% have been omitted – these included the courts and emergency services (3% each), law enforcement/crime prevention services (2% each) and 2% other responses. 2% were unable to answer, but no-one responded 'none'

Q. Which organisation or organisations, if any, do you think should have access to what has been recorded on CCTV cameras?

14.3 APPROPRIATE POSITIONING OF CCTV CAMERAS

When asked where it would be appropriate to place CCTV cameras, 9% were happy to place them anywhere with the exceptions of residential homes, bathrooms and changing places. Once again, no respondents said that CCTV cameras should **not** be placed anywhere, even those who showed concerns about them. Overall, Australians nominated two places each.

Chart 38. Places where it is appropriate for CCTV cameras to be installed



Q Where it is appropriate to have CCTV cameras?

Not only were Australians happy to nominate public spaces, but also 29% nominated private institutions including banks, entertainment venues, pubs and clubs. Support for placing CCTVs in private institutions increased with increasing age with people aged over 50 (32%) being significantly more likely than younger Australians (25% amongst those aged under 35) to suggest these venues. Across the country support was highest amongst Victorians and Tasmanians (35% and 39% respectively).

Support was fairly uniform across the country and by respondents of all types for positioning CCTV cameras in locations where people gather and may be at risk. While all respondents suggested placing CCTV cameras in Shopping Centres (28%), people living outside the main metropolitan areas (33%) and in the states of Tasmania (54%) and Queensland (36%) were the most likely to nominate these. People using public transport more than others (18 – 24 year olds (32%) and people living in metropolitan areas and the states of Victoria, New South

Wales and Western Australia) were the most likely to agree with placing CCTV cameras in stations, at bus or tram stops and at the airport. Respondents were more reticent to suggest placing CCTV cameras in public institutions such as government offices, hospitals, schools, police stations and the like.

APPENDIX 1

VERIFICATION STUDY

APPENDIX 1: VERIFICATION STUDY

A Verification Study was conducted to ensure that responses to questions in the main survey were accurate and representative of the broader community. Concerns had been raised in the past that contextual bias could enter the questionnaire as respondents were primed by previous questions to provide answers that may not have reflected their view when asked questions in isolation.

The Verification Study consisted of three questions from the main survey. It was conducted as part of NewsPoll's Omnibus, a multi-client survey, between 3 and 7 August 2007. The sampling structure of the Omnibus was similar to that used for the main survey and 1,200 Australians over 18 years of age were interviewed by telephone.

On the whole, responses were in line with the results of the main study except for the question on awareness of CCTV. This question was included because the following question on concerns about the use of CCTV in the main survey had only been asked of those who were aware of CCTV. There was a 22% discrepancy, with respondents of the Verification study (70%) being much less likely to be aware of CCTV than in the main survey (92%). One explanation for this is that respondents to the main survey answered the CCTV section last and were, by that point, quite attuned to privacy issues. In particular the 'privacy in the workplace' section had already asked about surveillance equipment. Also the introduction to the CCTV section was more detailed than the brief introduction in the verification study. The introductions were as follows:

Main Survey

The last topic I'd like your opinions on is Closed Circuit Television (CCTV). I'm talking about cameras that are used to monitor PUBLIC SPACE for example inner city streets, parks and car parks. Are you aware of or have you seen CCTV cameras?

Verification Survey

Thinking now about Closed Circuit Television, also know as CCTV Are you aware of or have you seen CCTV cameras?

With this exception, responses fell within the expected range of sampling error, including those relating to concern about the use of CCTV cameras.

Concern about personal information being sent overseas

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Very Concerned	63	66	3
Somewhat Concerned	27	23	-4
Not concerned	9	10	1
Don't know	1	1	0

Q. How concerned are you about Australian businesses sending their customers' personal information overseas to be processed?

Have been or know someone who has been the victim of identity theft or fraud

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Yes, you	9	8	-1
Yes, someone you know	17	14	-3
No	75	78	3
Don't know	<1	<1	0

Q. Now I'd like to ask you about identity fraud. By identity fraud and theft I mean where an individual obtains your personal information such as credit card, driver's licence, passport or other personal identification documents and uses these to obtain a benefit or service for themselves fraudulently. Have you, or someone you personally know, ever been the victim of identity fraud or theft?

Aware of CCTV cameras

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Yes	92	70	-22
No	7	29	22
Don't know	<1	2	0

Q. Thinking now about Closed Circuit Television, also know as CCTV. Are you aware of or have you seen CCTV cameras?

Concern about the use of CCTV cameras

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Very Concerned	3	5	2
Somewhat Concerned	11	12	1
Not concerned	85	83	-2
Don't know	<1	1	<1

Q. How concerned are you about the use of CCTV cameras in public spaces? Are you…?

APPENDIX 2

QUESTIONNAIRE

Wallis Consulting Group – Office of the Privacy Commissioner
2007 COMMUNITY ATTITUDES RESEARCH
FINAL QUESTIONNAIRE – 5th July

Good [Morning/ Afternoon/ Evening], my name is (SAY NAME) from Wallis Consulting Group. Today we are conducting an important survey on behalf of the Office of the Privacy Commissioner on the protection and use of people's personal information by businesses and other organisations. All views are of interest to us and results may be used to help better protect consumers' privacy in the future. Your answers will be strictly confidential and used as statistics only. The interview will take between 20 and 30 minutes on average depending on your answers and this is your chance to have your say on matters relating to privacy.

To ensure we speak to a representative sample of the population, we would like to speak with someone in the household aged 18 years or over.

IF NOT A CONVENIENT TIME NOW MAKE APPOINTMENT
IF ASKS HOW DID YOU GET MY NUMBER, SAY: Your number was selected randomly from the white pages phone book.

IF RESPONDENT WANTS FURTHER INFORMATION, SAY: You can find out more about this survey from our website (www.wallisgroup.com.au) or you may contact the Office of the Privacy Commissioner on 1300 363 992, during business hours.

This call may be monitored for quality control purposes. Is that OK with you?

Yes 1
No .....2 **MARK ACCORDINGLY**

We'd prefer that you answer all the questions, but if there are any that you don't want to answer, that's fine, just let me know.

S1 SEX. RECORD SEX OF RESPONDENT

MALE 1

FEMALE.....2

S2. Before we begin, to ensure we are interviewing a true cross-section of people, would you mind telling me which of the following age groups you belong to? (READ OUT)

18-24.....1
25-29.....2
30-34.....3
35-44.....4
45-49.....5
50-54.....6
55-64.....7
65+ 8
(DON'T READ) REFUSED .....9 ..Terminate

Check quotas

MAIN QUESTIONNAIRE

GENERAL ATTITUDES TO PROVIDING PERSONAL INFORMATION

Q1. Firstly, have you ever decided NOT TO DEAL with a PRIVATE COMPANY or CHARITY because of concerns over the protection or use of your personal information?

Yes.....1
No 2
CAN'T SAY 3

Q2. Have you ever decided NOT TO DEAL with a GOVERNMENT DEPARTMENT because of concerns over the protection or use of your personal information?

Yes.....1
No 2
CAN'T SAY 3

Q3. When completing forms or applications that ask for personal details, such as your name, contact details, income, marital status etc, how often, if ever, would you say you leave some questions blank as a means of protecting your personal information? Would that be …(READ OUT)?

Always.....1
Often 2
Sometimes.....3
Rarely.....4
Never 5
Can't say.....6

Q4. When providing your personal information to any organisation, IN GENERAL, what types of information do you feel RELUCTANT to provide? [IF NECESSARY For example, (ROTATE) your name, address, phone number, financial details, income, marital status, date of birth, email address, medical information, genetic information, or something else] What else?(MULTI)

If more than one

Q5. And of [LIST ANSWERS IN Q4] which ONE of these do you feel MOST RELUCTANT to provide? (SINGLE)

Name 1
Home Address 2
Home phone number 3
Financial details such as bank account 4
Details about your income 5
Marital status 6
Date of Birth 7
E-mail address 8
Medical history/health information 9
Genetic information 10
Religion 11
How many people or males in household/family member details 12
Other (Specify) 97
CAN'T SAY/ IT DEPENDS 98
None of these 99

IF MORE THAN ONE RESPONSE ON Q4, ASK:
IF MENTIONED TYPE OF INFORMATION, OR DEPENDS ON TYPE OF INFORMATION (CODES 1 TO 98 ON Q3), ASK:

Q6. And what is your MAIN reason for not wanting to provide your [ANSWER FROM Q5]?

May lead to financial loss/people might access bank Account 1
It's none of their business/Invasion of privacy 2
Discrimination 3
I do not want to be identified 4
I do not want people knowing where I live or how to Contact me 5
The information may be misused 6
Information might be passed on without my knowledge 7
Don't want junk mail/unsolicited mail. SPAM 8
I don't want to be bothered/hassled/hounded by phone Or door to door 9
For safety/security/protection from crime) 10
Unnecessary/irrelevant to their business or cause 11
Other (SPECIFY) 97

Can't say 98

ASK EVERYONE

Q7. Which of the following statements BEST DESCRIBES how you GENERALLY feel when organisations that you have NEVER DEALT WITH BEFORE send you unsolicited marketing information? Would you say...(READ OUT) (MULTI)?

I feel angry and annoyed 1

I feel concerned about where they obtained my personal information 2

It doesn't bother me either way, I don't care 3

It's a bit annoying but it's harmless 4

I enjoy reading the material and don't mind getting it at all 5

Fixed openend or something else (SPECIFY) 97

Fixed Single (DON'T READ) CAN'T SAY 98

TRUST IN ORGANISATIONS HANDLING PERSONAL INFORMATION

The next few questions concern the type of public information that should or should not be available to businesses for marketing purposes.

Q8 How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information? IF TRUSTWORTHY: Is that highly trustworthy or somewhat trustworthy? IF UNTRUSTWORTHY: Is that highly untrustworthy or somewhat untrustworthy?

ROTATE	Highly Trustworthy	Somewhat Trustworthy	Neither (DNR)	Somewhat untrustworthy	Highly untrustworthy	Can't say
a) Financial institutions	1	2	3	4	5	6
b)Real Estate Agents	1	2	3	4	5	6
c)Insurance Companies	1	2	3	4	5	6
d)Charities	1	2	3	4	5	6
e)Government Departments	1	2	3	4	5	6
f) Health service providers including doctors, hospitals and pharmacists	1	2	3	4	5	6
g)Market research organisations	1	2	3	4	5	6
h) Retailers	1	2	3	4	5	6
i) Businesses selling over the internet	1	2	3	4	5	6

ROTATE 9 and 9b

Q9 GENERALLY, how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive discounted purchases? Is that very or quite…

AND

Q9b. and how about if it meant you would have a chance to win a prize? Is that very or quite…

Very likely.....1
Quite likely 2
Neither likely or unlikely (DO NOT READ) 3
Quite unlikely 4
Very unlikely.....5
Can't say (DO NOT READ) 6
Depends (DO NOT READ).....7

LEVEL OF KNOWLEDGE

The next few questions are about the Federal Privacy Act and what you believe is covered by it.

Q10. Firstly, I'm going to list six types of organisations. Which of these, if any, do you think GENERALLY must operate under the Federal Privacy Act? (MULTI)

State Government departments 1
Commonwealth Government departments.....2
Small businesses.....3
Large businesses.....4
Charities.....5
None of them 6
Businesses based overseas.....7

Q11. Which of the following activities, if any, would be against the Federal Privacy Act? (RANDOM)

Your neighbours spying on you 1
An individual steals your ID and uses it to pretend that they are you 2
A small business reveals a customer's information to other customers 3
A large business reveals a customer's information to other customers 4
A bank or other organisation sends customer data to an overseas processing center..... 5

Q12. Were you aware of the Federal PRIVACY LAWS before this interview?

Yes.....1
No 2
Can't say.....3

Q13. If you wanted to report the misuse of your personal information, who would you be most likely to contact? (DO NOT READ OUT) Anyone else? (MULTI)

Police 1
Ombudsman 2
The organisation that was involved 3
The Privacy Commissioner (Federal or State) 4
Consumer Affairs (in your state)..... 5
Local State MP..... 6
State government department 7
Local Council 8
Lawyers/solicitors 9
Department of Fair Trading..... 10
The media eg TV/ radio/ newspapers..... 11
Seek advice from a friend or relative 12
Other (SPECIFY) 97
CAN'T SAY (if none) 98

ASK IF Q13 CODE 12

Q13a Is that friend or relative a professional in a relevant field?
What is it?

Police 1
Ombudsman 2
The organisation that was involved 3
The Privacy Commissioner (Federal or State) 4
Consumer Affairs (in your state)..... 5
Local State MP..... 6
State government department 7
Local Council 8
Lawyers/solicitors 9
Department of Fair Trading..... 10
The media eg TV/ radio/ newspapers..... 11
No 12
Other (SPECIFY) 97
CAN'T SAY (if none) 98

Q14. Are you aware that a Federal Privacy Commissioner exists to uphold privacy laws and to investigate complaints people may have about the misuse of their personal information?

Yes.....1
No 2
Can't say.....3

GOVERNMENT

The next questions cover Government Departments and privacy

Q15. If it was suggested that you be given a unique number to be used for identification by ALL Commonwealth Government departments and to use ALL government services, would you be in favour of this? Is that strongly or partly?

Strongly in favour 1
Partly in favour 2
Neither in favour or against it (DO NOT READ) 3
Partly against 4
Strongly against 5
Can't say (DO NOT READ) 6

Q16. Do you believe government departments should be able to cross-reference or share information in their databases about you and other Australians for:

Any Purpose 1
Some Purposes 2
Not At All 3
Can't Say.....4

IF SOME PURPOSES (CODE 2 IN Q16), ASK, OTHERWISE GO TO Q17:

Q16a For which of the following purposes do you believe governments should be allowed to cross reference your personal information? Should they be allowed to cross-reference information for…(READ OUT)

ROTATE	Yes	No	Don't know
Updating information like contact details	1	2	3
To prevent of solve fraud or other crime	1	2	3
To reduce costs or improve efficiency	1	2	3

ASK EVERYONE

Q17 Which of the following instances would you regard to be a misuse of your personal information?

ROTATE	Yes (invasion of privacy)	No	Don't know
a) a government department that you haven't dealt with gets hold of your personal information	1	2	3
b) a Government department monitors your activities on the Internet, recording information on the sites you visit without your knowledge	1	2	3
c) You supply your information to a Government department for a specific purpose and the agency uses it for another purpose.	1	2	3
d) A Government department asks you for personal information that doesn't seem relevant to the purpose of the transaction.	1	2	3

PRIVACY AND BUSINESSES

Q19. I would like you now to think about your privacy and businesses. I'm going to read you a number of statements and I'd like you to tell me whether you agree or disagree with each. Do you agree or disagree…(Is that strongly or partly

ROTATE	Strongly agree	Partly agree	Neither (DNR)	Partly disagree	Strongly disagree	Can't say (DNR)
a) businesses should be able to use the electoral roll for marketing purposes	1	2	3	4	5	6
b) businesses should be able to collect your information from the White Pages telephone directory without your knowledge for the purposes of marketing	1	2	3	4	5	6

Q18 Which of the following instances would you regard to be a misuse of your personal information?

ROTATE	Yes (invasion of privacy)	No	Don't know
a) a business that you don't know gets hold of your personal information	1	2	3
b) a business monitors your activities on the internet, recording information on the sites you visit without your knowledge.	1	2	3
c) You supply your information to a business for a specific purpose and the business uses it for another purpose.	1	2	3
d) A business asks you for personal information that doesn't seem relevant to the purpose of the transaction.	1	2	3

Q21. How concerned are you about Australian businesses sending their customers' personal information overseas to be processed? (READ OUT)

Very concerned.....1

Somewhat concerned.....2

Not concerned 3

Can't say.....4

HEALTH INFORMATION

The next few questions concern medical or health information and privacy.

Q22. When do you think your doctor should be able to share your health information with other doctors or health service providers, such as (ROTATE: pharmacists, specialists, pathologists or nurses)? (READ OUT)

For anything to do with my health care 1

Only for purposes that are related to the specific condition

Being treated 2

Only for serious or life threatening conditions 3

For no purpose, they should always ask for my consent. 4

Don't know/Can't say (DO NOT READ) 5

Q23. Do you agree or disagree that…?

Your doctor should be able to discuss your personal medical details with other health professionals - in a way that identifies you - WITHOUT YOUR CONSENT if they believe this would assist your treatment? Is that strongly or partly…

Strongly agree 1

Partly agree 2

Neither agree or disagree (DO NOT READ) 3

Partly disagree 4

Strongly disagree 5

Can't say (DO NOT READ) 6

Q24 The idea of building a National Health Information Network has been put forward. If this existed it would be an Australia-wide database which would allow medical professionals anywhere in Australia to access a patient's medical information if it was needed to treat a patient. The information could also be used on a de-identified basis to compile statistics on the types of treatments being used, types of illnesses suffered and so on…

If such a database existed, do you think inclusion of your medical information should be VOLUNTARY, or should ALL MEDICAL RECORDS be entered without permission or consent?

Inclusion should be voluntary 1

All medical records should be entered 2

Other (SPECIFY) 97

CAN'T SAY 98

Q25. Health information is often sought for research purposes and is generally de-identified - that is, NOT linked with information that identifies an individual. Do you believe that an individual's permission should be sought before their de-identified health information is released for research purposes, or not?

Yes.....1
No 2
Maybe 3
Can't say.....4

Q26. If a person has a serious genetic illness, under what circumstances do you think it is appropriate for their doctor to tell a relative so the relative could be tested for the same illness: Should doctors tell their relatives… (SINGLE) (READ OUT)

Without the patient's consent, even if it's unlikely that the relative may have the condition? 1
Without the patient's consent, but if there is strong possibility of the relative also having the condition? 2
If the patient consents to their relative being told 3
Don't know/ can't say (DO NOT READ). 4

EMPLOYEE PRIVACY

Now for a few questions about employees' privacy in the workplace

Q27. Do you think that employees should have access to the information their employer holds about them?

Yes.....1
No 2
Can't say.....3

Q28 I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing or not at all.

ROTATE	Whenever they choose	Only if suspect wrongdoing	Not at all	Can't say (DNR)
a) Read e-mails on a work e-mail account	1	2	3	4
b) Randomly drug and alcohol test employees	1	2	3	4
c) Monitor an employees work vehicle location (eg using GPS)	1	2	4	4

Q29a I'm going to read you another three statements. This time could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing, only for the safety or security of employees or not at all. (SINGLE)

ROTATE	Whenever they choose	Only if suspect wrongdoing	Safety/ Security	Not at all	Can't say (DNR)
a) Use surveillance equipment such as video and audio cameras to monitor the workplace	1	2	3	4	5
b) Monitor everything an employee types into their computer, including what web sites they visit and what they type in e-mails	1	2	3	4	5

Q29b And finally, do you think it's appropriate behaviour for an employer to monitor telephone conversations…?.(READ OUT).

Whenever they choose 1
Only if they suspect wrongdoing 2
For training and quality control; or 3
Not at all 4
Can't say (DO NOT READ) 5

Q30. How important is it to you that an employer has a privacy policy that covers when they will read employee emails, randomly drug test employees, use surveillance equipment to monitor employees and monitor telephone conversations. Is it ….(READ OUT)?

Not at all important 1
Not very important 2
Quite important 3
Very important 4
Can't say (DO NOT READ) 5

INTERNET

Now I'd like to ask you a few questions about using the internet and giving personal information over it.

Q31. Are you more or less concerned about providing your personal details electronically or online compared to in a hard copy/paper based format? …

More concerned 1
Less concerned 2
As concerned 3
Can't say (DO NOT READ) 4

Q32. And are you more or less concerned about providing your personal details electronically or online as opposed to over the telephone?

More concerned.....1
Less concerned 2
As concerned.....3
Can't say (DO NOT READ) 4

Q33. When completing online forms or applications that ask for personal details, have you ever PROVIDED FALSE INFORMATION as a means of protecting your privacy?

Yes.....1
No 2
Can't say 3

Q34. Are you MORE OR LESS concerned about the privacy of your personal information while using the internet than you were two years ago?

More concerned.....1
Less concerned 2
As concerned.....3
Can't say (DO NOT READ) 4

Q35. Do you normally read the privacy policy attached to any internet site?

Yes.....1
No 2
Can't say 3

IF SEEN OR READ PRIVACY POLICY (CODE 1 IN Q35), ASK, OTHERWISE GO TO Q27

Q36. What impact, if any, did seeing or reading these privacy policies have upon your attitude towards the site? **(DO NOT READ) (MULTI)**

It's a good idea/ I approve of the privacy policy/ they are doing the
Right thing/ prefer to see on sites/ respect sites for having it 1
Feel more confident/comfortable/secure/ about using site 2
Appear more honest/trustworthy/responsible/legitimate 3
Helps me decide whether to use the site or not 4
Still apprehensive about sites that have them/Don't trust them/ not convinced 5
Made me more cautious/aware when using the internet generally.....6
Too long/complicated to read 7
Other (Specify)..... 97
Can't say 98
None/no 99

ID THEFT

I'm now going to ask you a few questions about providing photo identification and identity fraud and theft. By identity fraud and theft I mean where an individual obtains your personal information (eg. credit card, drivers licence, passport or other personal identification documents) and uses these to fraudulently obtain a benefit or service for themselves.

Q37. Do you think it is acceptable that you need to *show* identification documents (such as a drivers license or passport) in the following situations: (MULTI - RECORD IF ANSWER YES - acceptable)

On entry to licensed premises (eg Pub/Club/Hotel 1
To obtain a credit card 2
To purchase general goods (eg clothing and food) 3
To purchase goods for which you need to be over 18 eg
Cigarettes 4
To get access to services 5

Q38 Do you think it is acceptable that *a copy* of your identification documents (such as a drivers license or passport) is made in the following situations:

On entry to licensed premises (eg Pub/Club/Hotel 1
To obtain a credit card 2
To purchase general goods (eg clothing and food) 3
To purchase good for which you need to be over 18 eg
Cigarettes 4
To get access to services 5

Q39 Have you (or someone you personally know) ever been the victim of identity fraud or theft?

Yes – it happened to me 1
Yes it happened to someone I personally know 2
No 3
Can't say 4

Q40 How concerned are you that you may become a victim of identity fraud or theft in the next 12 months? (READ OUT)

Very concerned 1
Somewhat concerned 2
Not concerned 3
Can't say (DO NOT READ) 4

Q41 Do you consider ID fraud or theft to be an invasion of privacy?

Yes 1
No 2
Can't say 3

Q42. What activities do you think most easily allow identity ID fraud or theft to occur? OPEN

CCTV

The last topic I'd like your opinions on is Closed Circuit Television (CCTV). I'm talking about cameras that are used to monitor PUBLIC SPACE for example inner city streets, parks and car parks.

Q43 Are you aware of or have you seen CCTV cameras?

Yes	1	
No	2	Go to Demos
CAN'T SAY	3	Go to Demos

Q44 How concerned are you about the use of CCTV cameras in public spaces, are you (READ OUT)…?

Very concerned	1
Somewhat concerned	2
Not concerned	3
Can't say	4

ASK IF CONCERNED

Q45 What is your main concern? (DO NOT READ)

Invasion of privacy	1
Information may be misused	2
It makes me uncomfortable	3
Other (specify)	4
Can't say	5

Q46**.** Which organisation or organisations, if any, do you think should have access to what has been recorded on CCTV cameras? (MULTI) (DO NOT READ)

Everyone	1
Police	2
Anti-terrorism law enforcement agencies	3
Local Councils	4
Government	5
Security companies	6
Businesses	7
The courts	8
The organisation that installed them	9
Other (specify)	10
Can't say	11

Q47. Where is it appropriate to have CCTV cameras?. OPEN (PROBE)

DEMOGRAPHICS

Finally, a few questions about yourself, just to ensure we have spoken to a representative cross section of people.

D1 What is the highest level of education you have reached?

Primary school 1
Intermediate (year 10) 2
VCE/HSC (year 12) 3
Undergraduate diploma/TAFE/Trade certs 4
Bachelor's Degree 5
Postgraduate qualification 6
CAN'T SAY 7

D2. Are you now in paid employment?
IF YES, ASK: Is that FULL-time for 35 hours or more a week, or part-time?
IF NO, ASK: Are you retired or a student?

Yes, Full-time 1
Yes, part time.....2
No, retired 3
No, student.....4
Other non-worker.....5
Refused.....6

ASK IF WORKING FULL/PART TIME
D3 Are you employed by someone else or are you an employer?

Employee 1
Employer.....2
Self-employed/SOHO 3
Both.....4
Can't say 5

D4. What is your (last) occupation?

(OPEN – code to ANZSCO standard)

D5. Which describes your household income before tax, best?

Less than $25,000 1
$25-75,000.....2
$75 - 100,000.....3
Over $100,000 4
Refused (do not read).....5

Closing Statements - All

Thank you very much for your time. Your views count and on behalf of the Office of the Privacy Commissioner and Wallis Consulting Group, I'm very glad you made them known. In case you missed it, my name is …... from Wallis Consulting Group. The information you have provided cannot be linked to you personally in any way.

If you have any queries about this study you can call the Australian Market and Social Research Society's free survey line on 1300 364 830.

Wallis

WALLIS CONSULTING GROUP PTY LTD
25 KING STREET MELBOURNE 3000 VICTORIA
TELEPHONE (03) 9621 1066 FAX (03) 9621 1919
A.B.N. 76 105 146 174
E-mail: wallis@wallisgroup.com.au

OFFICE OF THE PRIVACY COMMISSIONER, AUSTRALIA

COMMUNITY ATTITUDES TO PRIVACY 2007

METHODOLOGICAL REPORT

prepared for

Office of the Privacy Commissioner, Australia
Level 8, 133 Castlereagh Street
Sydney NSW 2000

August 2007
Reference Number: WG3322

2007 Australian Achiever® AWARDS
Highly Recommended
Excellence in Customer Service
1999-2007 inclusive

TABLE OF CONTENTS

1.0 SURVEY DESIGN 1

1.1 QUESTIONNAIRE DESIGN 1
1.2 SAMPLE DESIGN AND PREPARATION 4

2.0 SURVEY CONDUCT 5

2.1 QUESTIONNAIRE SET-UP AND TESTING 5
2.2 PILOT STUDY 5
2.3 MAIN STUDY 6
2.4 VERIFICATION STUDY 9

3.0 FIELD STATISTICS 10

3.1 RESPONSE RATE 10

4.0 POST SURVEY DATA MANAGEMENT 14

4.1 PREPARATION OF THE DATA 14
4.2 WEIGHTING OF THE SURVEY DATA 15
4.3 SAMPLE VARIANCE 17

5.0 DIFFICULTIES ENCOUNTERED, OBSERVATIONS AND RECOMMENDATIONS 18

5.1 THE QUESTIONNAIRE 18
5.2 FILLING QUOTAS 21
5.3 CONDUCT OF THE SURVEY – METHODOLOGY 22
5.4 PRACTICAL CONSIDERATIONS – THE TIMELINE 23
5.5 ANALYSIS OF THE SURVEY DATA 23

APPENDIX 1: VERIFICATION STUDY 24

APPENDIX 2: QUESTIONNAIRE 27

1.0 SURVEY DESIGN

1503 interviews were conducted using Computer Assisted Telephone Interviewing between 11 July and 7 August 2007. Respondents were chosen at random from household telephone numbers listed in the electronic White Pages. Quotas were placed on the sample by location, age and sex to ensure that sufficient interviews were conducted with representatives of these groups to allow robust analysis. The data was then weighted to reflect the Australian adult resident population as measured in the 2006 Australian Bureau of Statistics population Census.

In addition to the main study, a Verification Study was conducted in which three questions from the main study were asked on the NewsPoll Omnibus. The NewsPoll Omnibus was selected because the sample structure closely reflected the sample structure of the main survey. Interviewing occurred over the period 3 to 7 August 2007.

1.1 QUESTIONNAIRE DESIGN

The questionnaire was adapted from previous community attitudes surveys conducted in 2001 and 2004[1]. New modules on identity fraud and theft and closed-circuit television were added to the 2007 survey. These were developed jointly by Wallis Consulting Group (Wallis) and the Office of the Privacy Commissioner (the Office). The survey contained the following question modules:

- General Attitudes to Providing Personal Information
- Trust in Organisations Handling Personal Information
- Level of Knowledge
- Privacy and Government
- Privacy and Business
- Privacy and Health Information
- Privacy and The Workplace
- Identity Fraud and Theft
- Closed Circuit Television
- Demographics

[1] The 2001 and 2004 studies were conducted for the Office of the Privacy Commissioner by Roy Morgan Research.

In addition to these modules there was an introductory section which contained a brief statement of the purpose of the survey and contact details for the Office, Wallis and the Australian Market and Social Research Society's (AMSRS) survey line. This section also contained questions screening respondents for age and gender.

The following changes were made to the 2004 questionnaire for the purposes of the 2007 study:

- **Trust in Organisations Handling Personal Information** – respondents were no longer asked how trustworthy they thought *mail order companies* were, instead they were asked about *insurance companies*.
- **Level of Knowledge** – The question concerning which activities contravene the Act was completely different from 2004. Respondents were not asked to rate how much they thought they knew about protecting their personal information or to provide their views on organisations' general privacy policies.
- **Privacy and Business** – The questions concerning the use of the Electoral Roll and White Pages by business were moved into this section.
- **Privacy and Health Information** – Respondents were no longer asked whether they supported the idea of a unique identifier for health services. Instead they were asked about their support for a National Health database and, in addition, to suggest the circumstances under which it would be appropriate for a doctor to inform a relative of a person with a genetic illness that the person has the illness.
- **Privacy and the Workplace** – Responses to the statement about randomly drug testing employees were different and a multiple categories response was allowed. In 2004 one possible response was *only if necessary to ensure safety and security*, this was changed in 2007 to *only if they suspect wrongdoing.*
- **Demographics** – The narrow income bands that respondents had been asked to respond to in the past (leading to a 42% refusal rate) were reduced to four broad bands with a resultant fall in refusal rate to 19%. The income bands were reported slightly differently in 2007 to 2004, as a result, with households earning less than $25 000 roughly coinciding with those relying heavily on government benefits.

  The question ascertaining respondents' education levels had a slightly different response frame, offering less detail about the level of education completed up to Year 12 and including a post-graduate level of qualification.

Although the question about respondents' occupations was asked in exactly the same fashion as in previous surveys, a different approach to coding the responses was taken. Where interviewers coded the responses in previous surveys, in 2007 interviewers recorded occupation verbatim and responses were coded by a specialist coding team, therefore taking the onus off the interviewer.

The questionnaire was set up on Wallis' system and timed by interviewers. Their initial uninterrupted estimate of the length of the questionnaire was approximately 20 minutes, although there were concerns that this might be an underestimate. The individual question modules were timed and their order was changed to enhance flow and comprehension (as well as speed). Nonetheless, the pilot study revealed that 20 minutes was an underestimate, with an average time of just under 31 minutes being achieved. While it is common for pilot study interviews to run longer than when a survey goes live because interviewers are still familiarising themselves with the study and dealing with questions that respondents may have, as well as noting any problems or wording difficulties so that these may be improved, it was clear that this questionnaire could not run for 20 minutes as planned. The pilot showed that one of the key reasons that the interview was running longer than estimated was the interest respondents displayed in the subject matter. This meant those agreeing to interview were happy to deliberate on their responses to an extent unforeseen by our interviewing team in practice runs.

At the time of the pilot the question modules were timed as follows:

- Introduction – including screening and respondent selection – 1.5 minutes
- General Attitudes to Providing Personal Information – 2 minutes
- Trust in Organisations Handling Personal Information – 2 minutes
- Level of Knowledge – 2 minutes
- Privacy and Government – 1.5 minutes
- Privacy and Business – 1.5 minutes
- Privacy and Health Information – 4 minutes
- Privacy and the Workplace – 2.5 minutes
- Identity Fraud and Theft – 2 minutes
- Closed Circuit Television – 1.5 minutes

Wallis suggested several strategies for shortening the questionnaire including modularising the questionnaire so that all respondents would be asked 20 minutes' of questions. The Office decided to run the longer questionnaire and to change the introductory script accordingly to give respondents an accurate estimate of the time the interview would take to complete – in keeping the AMSRS Code of Professional Behaviour.

1.2 SAMPLE DESIGN AND PREPARATION

The sample was structured to reflect the population as well as ensure that there were enough respondents in each broad analysis group to facilitate statistical analysis. The sample was stratified by state and location with quota targets applied on age and location. A sex quota was not imposed, however the plan was to manage the ratio during fieldwork to ensure that the final outcome was no greater than 60:40 female:male (the final ratio was 55:45 female:male).

Table 1. Interviews achieved by quota cell

Sex	Age	Total	SYD	NSW/ ACT	MEL	VIC	BRIS	QLD	ADEL	SA/NT	PERTH	WA	TAS
Male	18-24	**74**	12	13	27	3	8	4	3	0	3	0	1
Male	25-34	**157**	40	17	33	7	22	11	7	3	11	3	3
Male	35-49	**194**	55	29	34	12	11	19	6	7	11	5	5
Male	50+	**245**	51	36	24	22	20	25	20	10	24	7	6
Female	18-24	**91**	15	10	29	1	8	11	4	0	10	3	0
Female	25-34	**222**	45	29	50	11	24	25	8	5	14	5	6
Female	35-49	**232**	50	30	39	14	18	27	12	10	9	12	11
Female	50+	**288**	47	46	34	20	24	28	30	13	23	10	13
Total		**1503**	**315**	**210**	**270**	**90**	**135**	**150**	**90**	**48**	**105**	**45**	**45**

The sample was drawn from the electronic White Pages allowing 60 numbers for each completed interview (90 000 in all). These numbers were checked for duplicates and missing digits which reduced the usable starting sample by about 5%. This list was washed against Wallis' internal *Do-Not-Call List* and a couple of numbers were removed. Following these processes, 84 157 numbers were available for use in the study, although not all numbers were used in the course of interviewing (see Field Statistics for more details).

2.0 SURVEY CONDUCT

2.1 QUESTIONNAIRE SET-UP AND TESTING

Once the questionnaire had been approved by the Office to proceed to pilot testing, it was set up on Wallis' CATI system and subjected to the following checking process:

- Wording, skips and routing were checked in hard-copy format.
- The questionnaire was checked by the analyst who set it up.
- The consultant checked the main skips by comparing top-line results from test interviews against the paper questionnaire.
- 'Dummy' interviews were conducted using automatic computer generated responses, and the top-line data from these were investigated to ensure all questions had the correct number of responses.
- A final test was run by a member of the fieldwork team prior to briefing and 'going live'.

2.2 PILOT STUDY

The pilot study was conducted as an exact copy of the main survey. This consisted of 22 interviews, two (one male and one female) in each of the eleven locations used to identify Australian regions and to be used to control quotas. This structure was used to test that the quotas were working correctly.

5 interviewers received a one-hour briefing on 28 June prior to conducting a test run and then live interviews. The interviews were completed on the evening of 29 June and interviewers were then debriefed.

The average duration of the questionnaire during the pilot was 30.6 minutes and a strike rate of 0.83 was achieved. This was clearly too long and the design procedures described earlier were introduced in order to shorten the length of the questionnaire.

There being no other changes to the questionnaire, the pilot study interviews were included with interviews from the main survey.

2.3 MAIN STUDY

A further 1481 interviews (making a total of 1503) were completed between 11 July and 7 August 2007. In addition to the interviewers who worked on the pilot study, 69 interviewers were briefed for the task and the interview was administered in exactly the same way as the pilot study.

2.3.1 Interviewers and field staff briefing

Interviewers, supervisors and senior field staff attended briefing sessions conducted by the Project Director or Project Manager. A total of 74 interviewers were briefed, as well as 5 supervisors. The Field Manager did not attend formal briefings but was briefed informally and attended progress meetings throughout the fieldwork.

Although a 'hard' copy of the questionnaire was available to interviewers, our briefing facilities allowed a projected image of a 'dummy' test interview to be used. The briefing session was interactive and interviewers took an active part in asking and answering questions as they were displayed on screen. This is much closer to the interviewers' real experience of the questionnaire than is the hard copy version.

Interviewers were able to ask questions and provide comment as they saw fit. Following the briefing interviewers conducted test interviews using an exact copy of the live questionnaire version on the CATI system to familiarise themselves with the practical use of the questionnaire before they conducted any live interviews.

In addition to briefing interviewers about the background of the study and its conduct, interviewers were briefed so that they could answer the following questions appropriately:

Q. How did you get my telephone number?

A. Your number was selected at random from the electronic White Pages.

Q. How do I know that my answers will remain confidential?

A. We will separate your telephone number, and any other identifiable information, from your answers to the survey as soon as the survey is complete. We will keep a record that we contacted this number for a period of six weeks and then delete the record.

Q. What will you do with my information?

A. Your answers, along with those of other respondents, will form the basis of a report submitted to the Office of the Privacy Commissioner. All analysis will be done on aggregated results – that is groups of people rather than individuals.

Interviewers were also given contact phone numbers for the Office in addition to the standard industry information line and reference to Wallis' website. More information about calls to these numbers is given in section 2.3.5.

2.3.2 Auditing and Quality Control

A total of 271 (18%) interviews were monitored by senior field staff on the CATI system; they could hear the call as well as see how interviewers were recording responses. Of those:

- 150 (10%) were *monitored* for a period less than 75% of the entire interview length; and
- 121 (8%) were *validated* by listening to more than 75% of the entire interview.

No issues with the survey were encountered through this process.

2.3.3 Security access control and privacy measures

Although no information that could personally identify individual respondents was captured in the course of this survey, Wallis often conducts such studies and has the requisite security in place.

As a primary security measure, Wallis has separated its day-to-day office network, which is accessible via e-mail and Internet, from its field operations. Identified information is only stored on the field system. The only identifying record captured in this survey was a household telephone number.

2.3.4 Call protocols

The Office had particular guidelines which were followed in the conduct of the survey. They were:

- No calls to be made on a Sunday unless by respondent request.
- Calls to be made within the hours of 9.00 am to 8.30 pm local time Monday to Friday and 9.00 am to 5.00 pm on Saturdays.

- If no contact had been made with a household after trying the number five times, no further attempt was made to contact anyone on that number.
- Appointments were only made if they were firm appointments. Interviewers did not make appointments without confirming a time with the respondent.

It should also be noted that Wallis does not leave messages on answering machines unless specifically requested to do so. In the conduct of this survey no messages were left on answering machines.

2.3.5 Calls to information numbers

For this study, respondents were given the option of checking on the bona fides of Wallis though the AMSRS industry information line or the company website. In addition, the survey bonafides could be checked via the Office's 1300 number or its website.

2.3.5.1 AMSRS SurveyLine (1300 364 830)

As Wallis is a member of the Association of Market and Social Research Organisations (AMSRO) and its consultants are members of the professional body, the AMSRS, respondents were directed to the industry hotline if they wished to check on the bona fides of Wallis or the conduct of the survey. The hotline is manned 24 hours a day. All calls, their nature and, if necessary, the resolution of them are logged. For this survey the AMSRS officer noted that there were no calls to the survey line relating to Wallis or the topic of privacy during the interviewing period.

2.3.5.2 The Office (1300 363 992)

The Office received three calls to its 1300 number, all related to the *bona fides* of the survey.

2.3.5.3 Wallis' Website (www.wallisgroup.com.au)

Respondents were provided with Wallis' website address. Surveys that are in field are logged on a page of this website (with ongoing and large-scale studies being given their own pages as required). This study did not receive its own page, but the following listing for the duration of the survey. We are unable to say how many people looked at the specific details of the survey on the website.

Community Attitudes Towards Privacy - The Office of the Privacy Commissioner

Similar studies have been carried out at regular intervals since 1990 in order to measure changes in public attitudes towards privacy-related concerns. This study investigates people's views about the way their privacy is handled in a range of areas including: health; work; business; and government. It asks respondents about such topics as privacy laws, ID theft, CCTV as well as the extent to which they trust organisations of different types. The Privacy Commissioner will use the results to suggest appropriate changes to privacy legislation for a review being carried out by the Australian Law Reform Commission.

1500 interviews will be completed with a representative sample of the adult Australian population. Interviews will be conducted from the 11th to the 21st July.

To check on these or any other surveys, please call AMSRS SurveyLine on 1300 364 832 or Wallis Consulting Group (03) 9621 1066.

2.4 VERIFICATION STUDY

A small study was conducted concurrently to ensure that responses to questions in the main survey were accurate and representative of the broader community. Concerns had been raised in the past that contextual bias could enter the questionnaire as respondents were primed by previous questions to provide answers that may not have reflected their view when asked questions in isolation.

Three questions were chosen from the main survey to be added to NewsPoll's Omnibus, a multi-client survey, between 3 and 7 August 2007. The sampling structure of the Omnibus was similar to that used for the main survey and 1200 Australians over 18 years of age were interviewed by telephone. Full details of this study are reported in Appendix 1.

3.0 FIELD STATISTICS

3.1 RESPONSE RATE

Tables 2 and 3 below outline the field statistics for the 2007 survey. The response rate for the survey was low with only one in twenty eligible respondents completing an interview. The principal reasons for this were:

- The length of the survey – respondents were told that the survey would take 20 to 30 minutes to complete and many were unable to spare that amount of time. This was particularly true of the younger age groups. The effective response rate was calculated from interviews achieved versus the telephone numbers in scope, excluding those who were ineligible (1503/28 262).
- The high number of younger respondents required to meet quota targets meant that some older willing respondents were not interviewed. Prior to quotas filling the response rate was much higher, as all willing respondents were able to participate.

The effective response rate thus differs markedly from the co-operation rate. This measure compares the number of in-scope respondents who were willing to participate (7188) to the total number interviewed (1503) and was 22% or similar to other population surveys conducted by Wallis.

While the low response rate is a concern, the characteristics of the final sample match the known characteristics of the Australian population well, therefore limiting the potential for sample bias and eliminating the need for substantial weighting to be applied to make the results representative. The differences are elaborated on in section 4.0.

The results of the verification study also match the main study closely suggesting that there was no notable sample bias.

Although statistics are not collected as to the reasons why respondents do not wish to participate, anecdotal evidence from field management staff suggests that the length of the survey was the primary reason for respondent refusal. Reportedly many respondents said that they would have participated if the survey had been shorter and interviewers cited high levels of interest in the subject matter. The market research industry guidelines on telephone interviewing length suggest that a maximum average interview length of 20 minutes, is appropriate where a prize or incentive is not offered (up to 40 minutes with a prize or

incentive). These guidelines are based on known industry response rates and evidence from surveys of non-response (see www.yourviewscount.com.au).

Table 2. Field Statistics[2] - Total attempted contacts

Total sample prepared	**84,157**
Used phone numbers	**57,516**
Unused sample (no call attempts)	**26,641**
RESOLVED	
In scope	
Interviews	**1,503**
Respondent not available in survey period	554
Stopped interview - not completed	21
Refusals (total)	26,184
Ineligible/ Does not qualify	5,131
Total in scope	**33,393**
Out of scope	
Business/ workplace number	765
FAX	1,080
Number disconnected	9,098
Total out of scope	**10,943**
Total Resolved Contact Attempts	**44,336**
Overall Effective Response Rate	**5%**
Change phone number*	11
UNRESOLVED	
Called 5 times - no answer on last attempt	6,439
No answer	4,153
Answering machine	2,238
Busy/Engaged	350
Total Unresolved Contact Attempts	**13,180**
Total Contact Attempts	**57,516**

**Some respondents made an appointment to be called on a different number to the one in the sample. The outcomes of these calls are included in the 'In-scope' statistics*

[2] Resolved contact attempts are those for which an outcome was achieved, either an interview, refusal or confirmation that the phone number was not in scope/respondents were ineligible. Unresolved contact attempts are those that did not result in contact with a respondent or confirmation that the phone number was not in scope.

Note that contact attempts refer to the outcome for each individual phone number called, total calls made refers to all call attempts – that is a single phone number may have been contacted more than once.

In total, the automatic dialler system made 118 581 call attempts to the 57 516 numbers used. The dialler stopped 66 933 calls without need to pass them to an interviewer because the system detected that the number was out of service, not being answered or was busy/engaged. Out of service numbers were discarded from the sample, but other numbers were called again up to a maximum of five times before being discarded. Calls that were detected as being connectable were passed to an interviewer. There were 51 648 such calls. Many of these calls resulted in connections to facsimile or answering machines and were terminated manually by interviewers. Table 2 shows the combined results of the call outcome statistics produced by the automatic dialling system and the interviewing system for the 57 516 numbers used. Table 3 details the outcomes of each call attempt.

Table 3. Field Statistics – Total calls made

Total calls made	**118,581**
Interviewer handled calls	
Interview	1,503
Answering machine	12,308
Respondent not available during survey period	554
Business/ workplace number	765
Refused - household	24,484
Refused - selected respondent	1,700
Ineligible/Does not qualify	5,131
FAX	1,080
Appointment	4,018
Change phone number	11
Stopped interview	94
Total interviewer handled calls	**51,648**
Dialer handled calls	
Dialer - Busy	3,238
Dialer - No answer	54,575
Dialer - Site out of service	9,120
Total dialer handled calls	**66,933**

Chart 1. Interviews achieved by number of calls to number

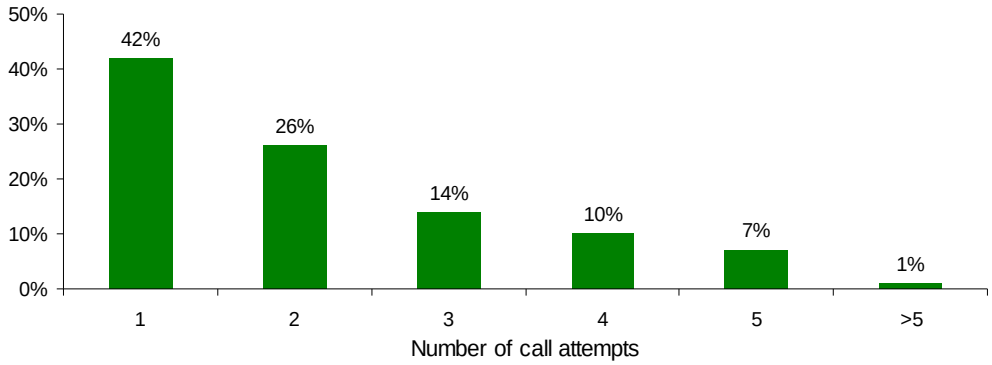


Chart 1 bears testimony to the wisdom of the Office's policy on restricting the number of calls to be made to each number in order to make contact to 5. 68% of interviews were achieved on the first or second call attempt. A small number of contacts were made on the sixth attempt. These were made where the fifth attempt resulted in a contact and a hard appointment being made for an interview at a later time.

4.0 POST SURVEY DATA MANAGEMENT

4.1 PREPARATION OF THE DATA

4.1.1 Data Analysis

Following the completion of interviewing, data analysts prepared a set of topline findings from which table specifications were formulated. A data specification request was prepared for the Data Analyst. They also reviewed the data file to ensure that it was complete and that answers were logical. Verbatim responses were removed from the data file and sent to be coded and re-input, in numeric form, back into the data file later.

In this case it had been agreed with the Office that all key demographic variables, namely age, location (state and metropolitan/non-metropolitan), sex, occupation, socio-economic standing, household income and education level, would be analysed. The topline findings guide the way in which analysis is conducted. For example, sex has only two possible answers, male and female, and both were represented in sufficient numbers to be able to compare these two subgroups. However, there were 11 occupation categories – too many to compare each to the other with any level of statistical veracity. For data analysis purposes these 11 categories were collapsed into 6 main categories. A set of detailed cross tabulations and a data file have been prepared.

4.1.2 Coding

Verbatim responses are assigned codes based on codeframes developed by the Project Director, Project Manager and the Coding Manager. In this case, they were based on those used in 2004 with additions as necessary. New questions were assessed to determine the key number of responses by major themes and these were approved by the Office for use by the coding team.

4.2 Weighting of the Survey Data

4.2.1 Profile of Respondents

Table 4 shows unweighted survey response data compared with the characteristics of the adult Australian population from the Australian Bureau of Statistics 2006 Census, to which they were weighted for age, sex and location. Note that 2001 Census data is shown for comparative purposes for occupation and education as 2006 data is not yet available.

Table 4. Respondent characteristics unweighted and weighted

	Unweighted Sample n=1503 %	Weighted to ABS Population Census n= 15 090 000 %
Sex		
Male	45	49
Female	55	51
Household Income		
Less than $25,000	16	19
$25,000 - $75,000	35	40
$75,000 - $100,000	13	13
Over $100,000	18	16
Refused	19	11
Occupation		
Upper White Collar	37	39
Lower White Collar	40	38
Upper Blue Collar	8	12
Lower Blue Collar	8	8
Don't know/other/refused	7	2
Education *		
Up to Year 12	38	53
Diploma/Trade	25	16
Degree of higher	36	19
Don't know/other	1	11

**NOTE: ABS data is not available from a single source, these figures are derived from two sources*

Although there were no quotas applied to household income, the distribution is similar to that shown in ABS 2006 Census data. The distribution in the sample is slightly skewed towards higher incomes and the refusal rate was 8% higher than non-reported or partially reported incomes. This is unlikely to lead to sample bias as the skew is very slight. Furthermore, 19% of respondents refused to answer the question in the survey and 11% refused to give their income details to the Australian Bureau of Statistics. As a result, it is impossible to tell what the actual distribution of household income is. However, in comparison to 2001 and 2004, a lower refusal rate was obtained in the survey, thus the income of a higher proportion of respondents is known.

Occupations were skewed towards *professionals and managers* (upper white) and away from *skilled and semi-skilled* occupations. However in aggregate, there is a good match between the categories.

Education level groups are captured slightly differently from previous surveys. The major difference is that respondents who completed up to and including Year 12 have been grouped together. Within this group attitudes are similar and contrast with people educated to other education levels. It is difficult to make accurate comparisons with the Australian public as the Australian Bureau of Statistics has not collected directly comparable data until 2006 and this data was not available at the time of writing this report. However, combining data on schooling level with education level overall, it seems that the sample is skewed quite heavily towards respondents with a degree or higher level of education.

4.3 SAMPLE VARIANCE

The sample variation at the national level (n=1503) is between 1.1% and 2.5%. This means that there is a 95% chance that if the survey was replicated and all things were equal, the results for any measure would fall within ± 2.5% of the survey estimate.

Throughout this survey comments have been made on results that are significant at the 95% confidence level. This is, in 95 out of 100 cases, the result would be within the expected range for the results shown. As a guide, to be statistically significant the percentage differences for the major analytical subgroups are:

- Age ± 6 – 9%
- Sex ± 5%
- State ± 7 – 17%
- Education level ± 6 – 7%
- Income ± 7 – 10%

The base sizes shown throughout the report are the actual number of respondents interviewed. The data on which the results are based are weighted.

5.0 DIFFICULTIES ENCOUNTERED, OBSERVATIONS AND RECOMMENDATIONS

Generally speaking, the survey went to plan. There were several exceptions relating to the questionnaire itself, filling the quotas, the mode of interviewing and the timeline allowed, especially for reporting. We elaborate on these difficulties further here and offer some thoughts as to ways in which these could be minimised in future studies.

5.1 THE QUESTIONNAIRE

5.1.1 Questionnaire length

The key problem with the questionnaire is its length. While it averaged just over 27 minutes, some interviews lasted for nearly 45 minutes. In some ways this is testament to the interest shown by respondents. As the field statistics show, only 21 people started the interview but failed to complete it and not all of these for reasons of length. Once respondents had agreed to interview having been told exactly how long it would take, they were committed to the task at hand.

The subject matter is clearly not a problem. If it were one would expect the quality of response to deteriorate as the interview progresses. There is no evidence for this and the level of refusal and "don't know" responses did not increase throughout the interview. In fact the reverse was true with 92% of respondents claiming to be aware of closed-circuit television and answering the subsequent questions about CCTV cameras – compared with only 70% in the Verification Study.

Having said this, the response rate was very low and this was directly related to respondents realising how much time they needed to give to participate – more time than most of them had available in the early to mid evening or during the day on Saturday.

As mentioned earlier, the market research industry guidelines on interview length recommend a maximum telephone interview length of 20 minutes where a prize or incentive is not offered and 40 minutes where a prize or incentive is offered. These guidelines are based on much academic research that demonstrates that respondent goodwill falls dramatically after 20 minutes of questioning on the telephone on average. It is possible that offering an incentive might increase response rates. We considered this idea, however rejected it because it was the wish of the Office that interviews should be totally anonymous – offering a prize or other incentive requires personal details in the form of a name and contact address to be captured.

It is also difficult to find an appropriate incentive for a project such as this one. Incentives usually consist of such items as games of chance (entry into a prize draw, a scratch and win ticket, etc.) or cash or kind. In both cases, not only does the actual choice of incentive become important, but also the administration adds substantially to the cost.

We believe a better way would be to modularise the questionnaire. This could be achieved in one of two ways.

- A core set of questions could be asked of all respondents and other topics could be allocated according to a rotation plan so that enough respondents answer questions on each topic to answer them reliably. If adopting this approach we would recommend using questions that vary by subgroup as the core, so that the maximum number of interviews is achieved for these and rotating modules that Australians have unanimous views about.
- All question modules could be rotated.

The drawback to this plan is that the rotation must be structured to allow enough people to answer each question module to provide robust answers. This may mean increasing the size of the sample. Nonetheless, if a questionnaire can be developed that takes no more than 20 minutes to complete, we believe that the additional costs involved in increasing the sample may well be offset by the improvement in response rate. Further, while the industry is adopting the 20-minute rule as a guideline at present, there are moves to mandate this in the near future. Companies that are members of AMSRO, as most credentialed research companies are, will be bound to comply. Thus paying incentives for telephone interviews that average over 20 minutes is likely to become compulsory before the Office conducts its next survey.

5.1.2 Question structure

Several of the questions in the questionnaire allowed respondents to offer a multiple response when a single response would make more sense. For the sake of comparability with the past, Wallis and the Office asked one question in the same fashion in 2007 as 2004, and two questions where the response codes had been altered allowed multiple responses, that had previously been asked as single responses on a different answer set. The following questions would benefit from allowing a single response only (the questionnaire appears in Appendix 2 and the question numbers below correspond to this questionnaire). We have also suggested some wording changes to make them easier for respondents to answer.

Q7 *Which of the following statements BEST describes how you generally feel when organisations that you have NEVER DEALT WITH BEFORE send you unsolicited marketing information? Would you say… (READ OUT)*

Allow only a single response – currently (and in 2001 and 2004) a multiple response is allowed and some people profess both to being *angry and annoyed* when they receive the material as well as *feeling concerned about where they obtained my personal information*

Q22 When do you think your doctor should be able to share your health information with other doctors or health service providers such as (ROTATE: pharmacists, specialists, pathologists or nurses)?

Responses to this question, which was established as a multiple response question, show that different health professionals are regarded differently, prompting some respondents to accept information sharing between their doctor and some of the named professionals but not others. We recommend using a single response and removing the descriptor (i.e. ROTATE; pharmacists, specialists, pathologist or nurses), allowing respondents to talk in general terms about whether in principle they believe their doctor should discuss their details with health professionals that might be relevant to their particular health problem.

Q29a I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing, for the safety and security of all employees, or not at all?

Responses suggest that respondents interpreted this question in different ways, with some considering the advantages of an employer having surveillance in public places and to monitor people entering and exiting a building, that is, for the safety and security of staff, whereas others were considering the privacy implications of having surveillance equipment monitoring employee performance. These two themes caused the question to be answered in more than one way by several respondents, hence the total responses did not add to 100. It would be preferable to state the exact circumstances more clearly. For example, 29a might become:

(a) *"Use surveillance equipment such as video and audio cameras to monitor all activities in the workplace/ parts of the workplace where the public has access, etc*

And (b) "finally, do you think it's appropriate behaviour for an employer to monitor telephone conversations…(READ OUT) whenever they choose, only if they suspect wrong-doing, for training or quality control purposes or not at all?"

Respondents are used to phone calls with frontline staff being monitored for quality control and training purposes and support this. Depending on what this question is meant to capture it might be better to be more specific about the nature of the call being made for example, to exclude frontline service staff and focus on general calls. E.g. *When do you think it's appropriate behaviour for an employer to monitor telephone conversations other than those being made to a customer services or sales officer?*

5.2 FILLING QUOTAS

In an effort to capture the views of younger Australians, particularly those aged 18 - 24, a disproportionate number of interviews was completed with them. The survey results show that the 18 – 24 year age group knows the least about privacy legislation and it is safe to say they would therefore have a lower level of interest in the subject matter than other age groups. This, added to the length of the questionnaire, the difficulty in locating young people in the permissible interviewing hours, plus the increased use of mobile communications by this age group since the last survey, caused this quota to be far more difficult to fill than anticipated. This had a flow on effect to the overall response rate, as willing respondents in older age groups were not interviewed because enough interviews had already been completed with Australians in these age groups.

We do not advocate changing the quota structure. However the difficulty might be alleviated slightly by changing the introduction to the questionnaire and asking to speak with the youngest male aged over 18 in preference to others, then the youngest female.

The Office also requested that no interviewing should be conducted on Sunday in order to avoid any suggestion that the interview process was an imposition on people's privacy and in line with the Australian Communications and Media Authority's (ACMA) industry standard at that time. We have found that Sunday is a good day to locate younger respondents. Indeed the company provided field statistics to ACMA privately and via the AMSRO submission in support of market researchers being allowed to make unsolicited research calls on Sundays. In its final legislation, ACMA accepted the industry position and market researchers are now able to make unsolicited research calls on Sunday. While we applaud the strict calling

regime enforced by the Office, we suggest that falling in line with industry standards, that is, allowing unsolicited calls to be made on Sunday, would also help in filling this quota.

5.3 CONDUCT OF THE SURVEY – METHODOLOGY

The survey has been conducted by telephone using a sample drawn at random from the electronic White Pages. In our proposal for this study we discussed other options and came to the conclusion that this method still offers the best means of gaining a representative sample of community attitudes. However we also pointed out:

- The proportion of households with a connected landline is falling with households opting to use mobile technology and/or Voice over Internet Protocol (VoIP) including Skype in greater number.
- Younger people in particular are the least likely to have a landline telephone with a growing percentage of those households with landlines using them only to access the Internet.
- The proportion of households with Internet access and, within this, broadband connections is increasing.

Another confusing factor for this survey was the recent introduction of the telemarketing Do Not Call Register administered by ACMA. It is too early to say to what extent its introduction contributed to a disappointing response rate.

Taking these factors into account, in our opinion it would be worth considering conducting all or some of the survey online in future. The biggest challenge to moving the survey online either in part, for example simply with younger aged Australians or completely, will be access to a representative listing of the Australian population. In our opinion such lists do not exist currently. However, the situation in this field is changing rapidly and it is likely that the lists will be much improved in three years' time.

5.4 PRACTICAL CONSIDERATIONS – THE TIMELINE

The Office was working towards publishing the report from this study during Privacy Awareness Week (26 August – 1 September 2007). This was achieved. However, fieldwork took longer than anticipated owing to the difficulty in filling younger age quotas and this reduced the amount of time available for reporting.

The ideal timetable from the time of appointment of the consultant to the project if conducted in the same manner as this year would be:

Questionnaire development	2 weeks
Pilot test	1 week
Interviewing	3 weeks
Data preparation and preliminary analysis	1 week
Reporting to draft stage	3 weeks
Redrafts	2 weeks

5.5 ANALYSIS OF THE SURVEY DATA

In analysing survey data it became apparent that many sections of the Australian community hold similar views on a range of privacy related issues. Demographic variables alone do not always differentiate differences in opinion and it might be possible to segment the community on the basis of attitudes towards privacy. The statistical techniques that are usually used to effect market segmentation (typically factor analysis and cluster analysis) require question answers to be *scaled*, for example, extent of agreement (strongly agree, partly agree, neither agree or disagree, partly disagree, strongly disagree), rather than *binary* (eg yes or no).

Many of the survey questions are asked in a suitable manner to support these analyses, however some related questions are not. An analysis could be done on the existing data set, however, if segmentation analysis is considered to be useful, we recommend reviewing and revising the questions with this purpose in mind when the survey is conducted again.

APPENDIX 1

VERIFICATION STUDY

APPENDIX 1: VERIFICATION STUDY

A Verification Study was conducted to ensure that responses to questions in the main survey were accurate and representative of the broader community. Concerns had been raised in the past that contextual bias could enter the questionnaire as respondents were primed by previous questions to provide answers that may not have reflected their view when asked questions in isolation.

The Verification Study consisted of three questions from the main survey. It was conducted as part of NewsPoll's Omnibus, a multi-client survey, between 3 and 7 August 2007. The sampling structure of the Omnibus was similar to that used for the main survey and 1,200 Australians over 18 years of age were interviewed by telephone.

On the whole, responses were in line with the results of the main study except for the question on awareness of CCTV. This question was included because the following question on concerns about the use of CCTV in the main survey had only been asked of those who were aware of CCTV. There was a 22% discrepancy, with respondents of the Verification study (70%) being much less likely to be aware of CCTV than in the main survey (92%). One explanation for this is that respondents to the main survey answered the CCTV section last and were, by that point, quite attuned to privacy issues. In particular the 'privacy in the workplace' section had already asked about surveillance equipment. Also the introduction to the CCTV section was more detailed than the brief introduction in the verification study. The introductions were as follows:

Main Survey

The last topic I'd like your opinions on is Closed Circuit Television (CCTV). I'm talking about cameras that are used to monitor PUBLIC SPACE for example inner city streets, parks and car parks. Are you aware of or have you seen CCTV cameras?

Verification Survey

Thinking now about Closed Circuit Television, also know as CCTV. Are you aware of or have you seen CCTV cameras?

With this exception, responses fell within the expected range of sampling error, including those relating to concern about the use of CCTV cameras.

Concern about personal information being sent overseas

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Very Concerned	63	66	3
Somewhat Concerned	27	23	-4
Not concerned	9	10	1
Don't know	1	1	0

Q. How concerned are you about Australian businesses sending their customers' personal information overseas to be processed?

Have been or know someone who has been the victim of identity theft or fraud

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Yes, you	9	8	-1
Yes, someone you know	17	14	-3
No	75	78	3
Don't know	<1	<1	0

Q. Now I'd like to ask you about identity fraud. By identity fraud and theft I mean where an individual obtains your personal information such as credit card, driver's licence, passport or other personal identification documents and uses these to obtain a benefit or service for themselves fraudulently. Have you, or someone you personally know, ever been the victim of identity fraud or theft?

Aware of CCTV cameras

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Yes	92	70	-22
No	7	29	22
Don't know	<1	2	0

Q. Thinking now about Closed Circuit Television, also know as CCTV Are you aware of or have you seen CCTV cameras?

Concern about the use of CCTV cameras

Response	Privacy Survey 2007 %	Verification Study (NewsPoll Omnibus) %	Difference %
Very Concerned	3	5	2
Somewhat Concerned	11	12	1
Not concerned	85	83	-2
Don't know	<1	1	<1

Q. How concerned are you about the use of CCTV cameras in public spaces? Are you…?

APPENDIX 2

QUESTIONNAIRE

Wallis Consulting Group – Office of the Privacy Commissioner
2007 COMMUNITY ATTITUDES RESEARCH
FINAL QUESTIONNAIRE – 5th July

Good [Morning/ Afternoon/ Evening], my name is (SAY NAME) from Wallis Consulting Group. Today we are conducting an important survey on behalf of the Office of the Privacy Commissioner on the protection and use of people's personal information by businesses and other organisations. All views are of interest to us and results may be used to help better protect consumers' privacy in the future. Your answers will be strictly confidential and used as statistics only. The interview will take between 20 and 30 minutes on average depending on your answers and this is your chance to have your say on matters relating to privacy.

To ensure we speak to a representative sample of the population, we would like to speak with someone in the household aged 18 years or over.

IF NOT A CONVENIENT TIME NOW MAKE APPOINTMENT
IF ASKS HOW DID YOU GET MY NUMBER, SAY: Your number was selected randomly from the white pages phone book.

IF RESPONDENT WANTS FURTHER INFORMATION, SAY: You can find out more about this survey from our website (www.wallisgroup.com.au) or you may contact the Office of the Privacy Commissioner on 1300 363 992, during business hours.

This call may be monitored for quality control purposes. Is that OK with you?

Yes 1
No .....2 **MARK ACCORDINGLY**

We'd prefer that you answer all the questions, but if there are any that you don't want to answer, that's fine, just let me know.

S1 SEX. RECORD SEX OF RESPONDENT

MALE 1

FEMALE.....2

S2. Before we begin, to ensure we are interviewing a true cross-section of people, would you mind telling me which of the following age groups you belong to? (READ OUT)

18-24.....1

25-29.....2

30-34.....3

35-44.....4

45-49.....5

50-54.....6

55-64.....7

65+ 8

(DON'T READ) REFUSED ..... 9 Terminate

Check quotas

MAIN QUESTIONNAIRE

GENERAL ATTITUDES TO PROVIDING PERSONAL INFORMATION

Q1. Firstly, have you ever decided NOT TO DEAL with a PRIVATE COMPANY or CHARITY because of concerns over the protection or use of your personal information?

Yes.....1
No 2
CAN'T SAY 3

Q2. Have you ever decided NOT TO DEAL with a GOVERNMENT DEPARTMENT because of concerns over the protection or use of your personal information?

Yes.....1
No 2
CAN'T SAY 3

Q3. When completing forms or applications that ask for personal details, such as your name, contact details, income, marital status etc, how often, if ever, would you say you leave some questions blank as a means of protecting your personal information? Would that be …(READ OUT)?

Always.....1
Often 2
Sometimes.....3
Rarely.....4
Never 5
Can't say.....6

Q4. When providing your personal information to any organisation, IN GENERAL, what types of information do you feel RELUCTANT to provide? [IF NECESSARY For example, (ROTATE) your name, address, phone number, financial details, income, marital status, date of birth, email address, medical information, genetic information, or something else] What else?(MULTI)

If more than one
Q5. And of [LIST ANSWERS IN Q4] which ONE of these do you feel MOST RELUCTANT to provide? (SINGLE)

Name 1
Home Address 2
Home phone number 3
Financial details such as bank account 4
Details about your income 5
Marital status..... 6
Date of Birth 7
E-mail address 8
Medical history/health information 9
Genetic information..... 10

Religion 11
How many people or males in household/family member details 12
Other (Specify) 97
CAN'T SAY/ IT DEPENDS 98
None of these 99

IF MORE THAN ONE RESPONSE ON Q4, ASK:
IF MENTIONED TYPE OF INFORMATION, OR DEPENDS ON TYPE OF INFORMATION (CODES 1 TO 98 ON Q3), ASK:

Q6. And what is your MAIN reason for not wanting to provide your [ANSWER FROM Q5]?

May lead to financial loss/people might access bank
Account 1
It's none of their business/Invasion of privacy 2
Discrimination 3
I do not want to be identified 4
I do not want people knowing where I live or how to
Contact me 5
The information may be misused 6
Information might be passed on without my knowledge 7
Don't want junk mail/unsolicited mail. SPAM 8
I don't want to be bothered/hassled/hounded by phone
Or door to door 9
For safety/security/protection from crime) 10
Unnecessary/irrelevant to their business or cause 11
Other (SPECIFY) 97
Can't say 98

ASK EVERYONE

Q7. Which of the following statements BEST DESCRIBES how you GENERALLY feel when organisations that you have NEVER DEALT WITH BEFORE send you unsolicited marketing information? Would you say...(READ OUT) (MULTI)?

I feel angry and annoyed 1

I feel concerned about where they obtained my personal information 2

It doesn't bother me either way, I don't care 3

It's a bit annoying but it's harmless 4

I enjoy reading the material and don't mind getting it at all 5

Fixed openend or something else (SPECIFY) 97

Fixed Single (DON'T READ) CAN'T SAY 98

TRUST IN ORGANISATIONS HANDLING PERSONAL INFORMATION

The next few questions concern the type of public information that should or should not be available to businesses for marketing purposes.

Q8 How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information? IF TRUSTWORTHY: Is that highly trustworthy or somewhat trustworthy? IF UNTRUSTWORTHY: Is that highly untrustworthy or somewhat untrustworthy?

ROTATE	Highly Trustworthy	Somewhat Trustworthy	Neither (DNR)	Somewhat untrustworthy	Highly untrustworthy	Can't say
a) Financial institutions	1	2	3	4	5	6
b)Real Estate Agents	1	2	3	4	5	6
c)Insurance Companies	1	2	3	4	5	6
d)Charities	1	2	3	4	5	6
e)Government Departments	1	2	3	4	5	6
f) Health service providers including doctors, hospitals and pharmacists	1	2	3	4	5	6
g)Market research organisations	1	2	3	4	5	6
h) Retailers	1	2	3	4	5	6
i) Businesses selling over the internet	1	2	3	4	5	6

ROTATE 9 and 9b

Q9 GENERALLY, how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive discounted purchases? Is that very or quite…

AND

Q9b. and how about if it meant you would have a chance to win a prize? Is that very or quite…

Very likely.....1
Quite likely 2
Neither likely or unlikely (DO NOT READ) 3
Quite unlikely 4
Very unlikely.....5
Can't say (DO NOT READ) 6
Depends (DO NOT READ).....7

LEVEL OF KNOWLEDGE

The next few questions are about the Federal Privacy Act and what you believe is covered by it.

Q10. Firstly, I'm going to list six types of organisations. Which of these, if any, do you think GENERALLY must operate under the Federal Privacy Act? (MULTI)

State Government departments 1
Commonwealth Government departments.....2
Small businesses.....3
Large businesses.....4
Charities.....5
None of them 6
Businesses based overseas.....7

Q11. Which of the following activities, if any, would be against the Federal Privacy Act? (RANDOM)

Your neighbours spying on you 1
An individual steals your ID and uses it to pretend that they are you 2
A small business reveals a customer's information to other customers 3
A large business reveals a customer's information to other customers 4
A bank or other organisation sends customer data to an overseas processing center..... 5

Q12. Were you aware of the Federal PRIVACY LAWS before this interview?

Yes.....1
No 2
Can't say.....3

Q13. If you wanted to report the misuse of your personal information, who would you be most likely to contact? (DO NOT READ OUT) Anyone else? (MULTI)

Police 1
Ombudsman 2
The organisation that was involved 3
The Privacy Commissioner (Federal or State) 4
Consumer Affairs (in your state)..... 5
Local State MP..... 6
State government department 7
Local Council 8
Lawyers/solicitors 9
Department of Fair Trading..... 10
The media eg TV/ radio/ newspapers..... 11
Seek advice from a friend or relative 12
Other (SPECIFY) 97
CAN'T SAY (if none)..... 98

ASK IF Q13 CODE 12

Q13a Is that friend or relative a professional in a relevant field?
What is it?

Police 1
Ombudsman 2
The organisation that was involved 3
The Privacy Commissioner (Federal or State) 4
Consumer Affairs (in your state)..... 5
Local State MP..... 6
State government department 7
Local Council 8
Lawyers/solicitors 9
Department of Fair Trading..... 10
The media eg TV/ radio/ newspapers..... 11
No 12
Other (SPECIFY) 97
CAN'T SAY (if none) 98

Q14. Are you aware that a Federal Privacy Commissioner exists to uphold privacy laws and to investigate complaints people may have about the misuse of their personal information?

Yes.....1
No 2
Can't say.....3

GOVERNMENT

The next questions cover Government Departments and privacy

Q15. If it was suggested that you be given a unique number to be used for identification by ALL Commonwealth Government departments and to use ALL government services, would you be in favour of this? Is that strongly or partly?

Strongly in favour 1
Partly in favour 2
Neither in favour or against it (DO NOT READ) 3
Partly against 4
Strongly against 5
Can't say (DO NOT READ) 6

Q16. Do you believe government departments should be able to cross-reference or share information in their databases about you and other Australians for:

Any Purpose 1
Some Purposes 2
Not At All 3
Can't Say.....4

IF SOME PURPOSES (CODE 2 IN Q16), ASK, OTHERWISE GO TO Q17:

Q16a For which of the following purposes do you believe governments should be allowed to cross reference your personal information? Should they be allowed to cross-reference information for…(READ OUT)

ROTATE	Yes	No	Don't know
Updating information like contact details	1	2	3
To prevent of solve fraud or other crime	1	2	3
To reduce costs or improve efficiency	1	2	3

ASK EVERYONE

Q17 Which of the following instances would you regard to be a misuse of your personal information?

ROTATE	Yes (invasion of privacy)	No	Don't know
a) a government department that you haven't dealt with gets hold of your personal information	1	2	3
b) a Government department monitors your activities on the Internet, recording information on the sites you visit without your knowledge	1	2	3
c) You supply your information to a Government department for a specific purpose and the agency uses it for another purpose.	1	2	3
d) A Government department asks you for personal information that doesn't seem relevant to the purpose of the transaction.	1	2	3

PRIVACY AND BUSINESSES

Q19. I would like you now to think about your privacy and businesses. I'm going to read you a number of statements and I'd like you to tell me whether you agree or disagree with each. Do you agree or disagree…(Is that strongly or partly

ROTATE	Strongly agree	Partly agree	Neither (DNR)	Partly disagree	Strongly disagree	Can't say (DNR)
a) businesses should be able to use the electoral roll for marketing purposes	1	2	3	4	5	6
b) businesses should be able to collect your information from the White Pages telephone directory without your knowledge for the purposes of marketing	1	2	3	4	5	6

Q18 Which of the following instances would you regard to be a misuse of your personal information?

ROTATE	Yes (invasion of privacy)	No	Don't know
a) a business that you don't know gets hold of your personal information	1	2	3
b) a business monitors your activities on the internet, recording information on the sites you visit without your knowledge.	1	2	3
c) You supply your information to a business for a specific purpose and the business uses it for another purpose.	1	2	3
d) A business asks you for personal information that doesn't seem relevant to the purpose of the transaction.	1	2	3

Q21. How concerned are you about Australian businesses sending their customers' personal information overseas to be processed? (READ OUT)

Very concerned.....1

Somewhat concerned.....2

Not concerned 3

Can't say.....4

HEALTH INFORMATION

The next few questions concern medical or health information and privacy.

Q22. When do you think your doctor should be able to share your health information with other doctors or health service providers, such as (ROTATE: pharmacists, specialists, pathologists or nurses)? (READ OUT)

For anything to do with my health care 1
Only for purposes that are related to the specific condition
Being treated 2
Only for serious or life threatening conditions 3
For no purpose, they should always ask for my consent. 4
Don't know/Can't say (DO NOT READ) 5

Q23. Do you agree or disagree that…?

Your doctor should be able to discuss your personal medical details with other health professionals - in a way that identifies you - WITHOUT YOUR CONSENT if they believe this would assist your treatment? Is that strongly or partly…

Strongly agree 1
Partly agree 2
Neither agree or disagree (DO NOT READ) 3
Partly disagree 4
Strongly disagree 5
Can't say (DO NOT READ) 6

Q24 The idea of building a National Health Information Network has been put forward. If this existed it would be an Australia-wide database which would allow medical professionals anywhere in Australia to access a patient's medical information if it was needed to treat a patient. The information could also be used on a de-identified basis to compile statistics on the types of treatments being used, types of illnesses suffered and so on…

If such a database existed, do you think inclusion of your medical information should be VOLUNTARY, or should ALL MEDICAL RECORDS be entered without permission or consent?

Inclusion should be voluntary 1
All medical records should be entered 2
Other (SPECIFY) 97
CAN'T SAY 98

Q25. Health information is often sought for research purposes and is generally de-identified - that is, NOT linked with information that identifies an individual. Do you believe that an individual's permission should be sought before their de-identified health information is released for research purposes, or not?

Yes.....1
No 2
Maybe 3
Can't say.....4

Q26. If a person has a serious genetic illness, under what circumstances do you think it is appropriate for their doctor to tell a relative so the relative could be tested for the same illness: Should doctors tell their relatives… (SINGLE) (READ OUT)

Without the patient's consent, even if it's unlikely that the relative may have the condition? 1
Without the patient's consent, but if there is strong possibility of the relative also having the condition? 2
If the patient consents to their relative being told 3
Don't know/ can't say (DO NOT READ). 4

EMPLOYEE PRIVACY

Now for a few questions about employees' privacy in the workplace

Q27. Do you think that employees should have access to the information their employer holds about them?

Yes.....1
No 2
Can't say.....3

Q28 I'm going to read you three statements. For each could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing or not at all.

ROTATE	Whenever they choose	Only if suspect wrongdoing	Not at all	Can't say (DNR)
a) Read e-mails on a work e-mail account	1	2	3	4
b) Randomly drug and alcohol test employees	1	2	3	4
c) Monitor an employees work vehicle location (eg using GPS)	1	2	4	4

Q29a I'm going to read you another three statements. This time could you tell me if you think it's appropriate behaviour for an employer to do whenever they choose, only if they suspect wrong-doing, only for the safety or security of employees or not at all. (SINGLE)

ROTATE	Whenever they choose	Only if suspect wrongdoing	Safety/ Security	Not at all	Can't say (DNR)
a) Use surveillance equipment such as video and audio cameras to monitor the workplace	1	2	3	4	5
b) Monitor everything an employee types into their computer, including what web sites they visit and what they type in e-mails	1	2	3	4	5

Q29b And finally, do you think it's appropriate behaviour for an employer to monitor telephone conversations…?.(READ OUT).

Whenever they choose 1
Only if they suspect wrongdoing 2
For training and quality control; or 3
Not at all 4
Can't say (DO NOT READ) 5

Q30. How important is it to you that an employer has a privacy policy that covers when they will read employee emails, randomly drug test employees, use surveillance equipment to monitor employees and monitor telephone conversations. Is it ….(READ OUT)?

Not at all important 1
Not very important 2
Quite important 3
Very important 4
Can't say (DO NOT READ) 5

INTERNET
Now I'd like to ask you a few questions about using the internet and giving personal information over it.

Q31. Are you more or less concerned about providing your personal details electronically or online compared to in a hard copy/paper based format? …

More concerned 1
Less concerned 2
As concerned 3
Can't say (DO NOT READ) 4

Q32. And are you more or less concerned about providing your personal details electronically or online as opposed to over the telephone?

More concerned.....1
Less concerned 2
As concerned.....3
Can't say (DO NOT READ) 4

Q33. When completing online forms or applications that ask for personal details, have you ever PROVIDED FALSE INFORMATION as a means of protecting your privacy?

Yes.....1
No 2
Can't say 3

Q34. Are you MORE OR LESS concerned about the privacy of your personal information while using the internet than you were two years ago?

More concerned.....1
Less concerned 2
As concerned.....3
Can't say (DO NOT READ) 4

Q35. Do you normally read the privacy policy attached to any internet site?

Yes.....1
No 2
Can't say 3

IF SEEN OR READ PRIVACY POLICY (CODE 1 IN Q35), ASK, OTHERWISE GO TO Q27

Q36. What impact, if any, did seeing or reading these privacy policies have upon your attitude towards the site? **(DO NOT READ) (MULTI)**

It's a good idea/ I approve of the privacy policy/ they are doing the
Right thing/ prefer to see on sites/ respect sites for having it 1
Feel more confident/comfortable/secure/ about using site 2
Appear more honest/trustworthy/responsible/legitimate 3
Helps me decide whether to use the site or not 4
Still apprehensive about sites that have them/Don't trust them/ not convinced 5
Made me more cautious/aware when using the internet generally 6
Too long/complicated to read 7
Other (Specify)..... 97
Can't say 98
None/no 99

ID THEFT

I'm now going to ask you a few questions about providing photo identification and identity fraud and theft. By identity fraud and theft I mean where an individual obtains your personal information (eg. credit card, drivers licence, passport or other personal identification documents) and uses these to fraudulently obtain a benefit or service for themselves.

Q37. Do you think it is acceptable that you need to *show* identification documents (such as a drivers license or passport) in the following situations: (MULTI - RECORD IF ANSWER YES - acceptable)

On entry to licensed premises (eg Pub/Club/Hotel 1
To obtain a credit card 2
To purchase general goods (eg clothing and food) 3
To purchase goods for which you need to be over 18 eg
Cigarettes 4
To get access to services 5

Q38 Do you think it is acceptable that *a copy* of your identification documents (such as a drivers license or passport) is made in the following situations:

On entry to licensed premises (eg Pub/Club/Hotel 1
To obtain a credit card 2
To purchase general goods (eg clothing and food) 3
To purchase good for which you need to be over 18 eg
Cigarettes 4
To get access to services 5

Q39 Have you (or someone you personally know) ever been the victim of identity fraud or theft?

Yes – it happened to me 1
Yes it happened to someone I personally know 2
No 3
Can't say 4

Q40 How concerned are you that you may become a victim of identity fraud or theft in the next 12 months? (READ OUT)

Very concerned 1
Somewhat concerned 2
Not concerned 3
Can't say (DO NOT READ) 4

Q41 Do you consider ID fraud or theft to be an invasion of privacy?

Yes 1
No 2
Can't say 3

Q42. What activities do you think most easily allow identity ID fraud or theft to occur? OPEN

CCTV

The last topic I'd like your opinions on is Closed Circuit Television (CCTV). I'm talking about cameras that are used to monitor PUBLIC SPACE for example inner city streets, parks and car parks.

Q43 Are you aware of or have you seen CCTV cameras?

Yes	1	
No	2	Go to Demos
CAN'T SAY	3	Go to Demos

Q44 How concerned are you about the use of CCTV cameras in public spaces, are you (READ OUT)…?

Very concerned	1
Somewhat concerned	2
Not concerned	3
Can't say	4

ASK IF CONCERNED

Q45 What is your main concern? (DO NOT READ)

Invasion of privacy	1
Information may be misused	2
It makes me uncomfortable	3
Other (specify)	4
Can't say	5

Q46**.** Which organisation or organisations, if any, do you think should have access to what has been recorded on CCTV cameras? (MULTI) (DO NOT READ)

Everyone	1
Police	2
Anti-terrorism law enforcement agencies	3
Local Councils	4
Government	5
Security companies	6
Businesses	7
The courts	8
The organisation that installed them	9
Other (specify)	10
Can't say	11

Q47. Where is it appropriate to have CCTV cameras?. OPEN (PROBE)

DEMOGRAPHICS

Finally, a few questions about yourself, just to ensure we have spoken to a representative cross section of people.

D1 What is the highest level of education you have reached?

Primary school 1
Intermediate (year 10) 2
VCE/HSC (year 12) 3
Undergraduate diploma/TAFE/Trade certs 4
Bachelor's Degree 5
Postgraduate qualification 6
CAN'T SAY 7

D2. Are you now in paid employment?
IF YES, ASK: Is that FULL-time for 35 hours or more a week, or part-time?
IF NO, ASK: Are you retired or a student?

Yes, Full-time 1
Yes, part time.....2
No, retired 3
No, student.....4
Other non-worker.....5
Refused.....6

ASK IF WORKING FULL/PART TIME
D3 Are you employed by someone else or are you an employer?

Employee 1
Employer.....2
Self-employed/SOHO 3
Both.....4
Can't say 5

D4. What is your (last) occupation?

(OPEN – code to ANZSCO standard)

D5. Which describes your household income before tax, best?

Less than $25,000 1
$25-75,000.....2
$75 - 100,000.....3
Over $100,000 4
Refused (do not read).....5

Closing Statements - All

Thank you very much for your time. Your views count and on behalf of the Office of the Privacy Commissioner and Wallis Consulting Group, I'm very glad you made them known. In case you missed it, my name is …... from Wallis Consulting Group. The information you have provided cannot be linked to you personally in any way.

If you have any queries about this study you can call the Australian Market and Social Research Society's free survey line on 1300 364 830.

Australian Government

Office of the Australian Information Commissioner

Community Attitudes to Privacy survey

Research Report

2013

Protecting information rights — advancing information policy

THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER WOULD LIKE TO THANK THE FOLLOWING SPONSORS FOR THEIR SUPPORT OF THE COMMUNITY ATTITUDES TO PRIVACY SURVEY

Primary Sponsor

CommonwealthBank

Key Sponsor

HENRY DAVIS YORK

Sponsor

McAfee
An Intel Company

PREPARED FOR THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER BY

Wallis | strategic market & social research

The Office of the Australian Information Commissioner (OAIC) was established on 1 November 2010 by the *Australian Information Commissioner Act 2010*.

All OAIC publications can be made available in a range of accessible formats for people with disabilities. If you require assistance, please contact the OAIC.

ISBN 978-1-877079-76-4

Creative Commons

With the exception of the Commonwealth Coat of Arms, this report *Community attitudes to privacy survey, Research report 2013* is licensed under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/deed.en).

This publication should be attributed as: Office of the Australian Information Commissioner, *Community attitudes to privacy survey, Research report 2013* .

Enquiries regarding the licence and any use of this report are welcome at:

Office of the Australian Information Commissioner
GPO Box 2999
CANBERRA ACT 2601
Tel: 02 9284 9800
TTY: 1800 620 241 (no voice calls)
Email: enquiries@oaic.gov.au

TABLE OF CONTENTS

1.0 Summary of key findings 3

The survey 3

The findings 3

2.0 Background and objectives 7

Previous surveys 7

3.0 Methodology 9

Data collection 9

Sample — source and management 11

Questionnaire development 11

Pilot study 12

Weighting 12

Analysis 14

Definitions 14

4.0 Detailed findings 15

Awareness of Federal privacy laws 16

General attitudes towards privacy and personal information 17

Privacy problems and complaints 22

Trust 23

Personal responsibility 29

Medical and health information 30

Privacy in the workplace 32

Identification document scanning 34

Internet and smartphones 36

ID theft and fraud 43

Credit reporting 44

5.0 Appendix 1: Questionnaire 47

1.0 Summary of key findings

The survey

The 2013 Office of the Australian Information Commissioner (OAIC) Community Attitudes to Privacy study aims to measure Australians' changing awareness and opinions about privacy, as well as their expectations in relation to the handling of their personal information. The study also seeks views on a range of privacy issues, such as online privacy, credit reporting and privacy in the workplace.

The study has been conducted since 1990 and was last undertaken in 2007. All previous studies were conducted by telephone, and respondents were selected at random from an electronic listing of telephone numbers.

The number of Australians with a listed fixed line phone is declining and the proportion of younger Australians with a fixed line phone is even lower. Therefore, it was decided to conduct the 2013 study by telephone, but this time using lists of fixed line and mobile phones as well as numbers generated at random and checked against known live numbers. During July 2013, 1,000 Australians from a range of age groups, locations and backgrounds were contacted and agreed to participate.

Some questions asked in this study have been asked before and trend data are available. However, a number of questions were modified to reflect advances in technology as well as changes in privacy laws. In particular, questions relating to health information, online privacy, privacy in the workplace and ID theft and fraud were heavily modified. The survey includes a number of new questions, including questions about online tracking, smart phones, social networking, credit reporting and what actions people take to protect their own privacy.

The OAIC was keen to conduct the survey this year as the Australian public, businesses and government agencies prepare for significant changes to the *Privacy Act 1988* (Privacy Act) that are due to take effect from March 2014.

The findings

In the context of talking about personal information, Australians believe the biggest privacy risks facing people are online services — including social media sites. Almost a half of the population (48%) mentioned these risks spontaneously. A quarter (23%) felt that the risk of ID fraud and theft was the biggest, followed by data security (16%) and the risks to financial data in general (11%). Young Australians were most concerned about personal information and online services, with six in ten (60%) mentioning this as a privacy risk. There were other concerns, but none of the others were mentioned as a major risk by more than one in ten Australians.

This new, opening survey question gave context to the rest of the interview. The one in six (17%) Australians who regret something they have posted on a social networking site together with the increasing proportion of the population that has been affected by ID fraud and theft, or knows someone who has, have clearly been affected by their experiences. Two thirds (69%) are concerned that they may become a victim in the next year — a significant increase on the situation six years ago (60%). One third (33%) of Australians say that they have had problems with the way that their personal information was handled in the previous year.

Another trend that has no doubt served to underpin increasing caution amongst Australians is the increasing proportion of the population that is aware of Federal privacy laws (82% versus 69% in 2007). Presumably the public is also aware of other consumer protection laws, given the increased proportion of the community that has made a complaint about misuse of their personal information to a number of different ombudsmen, including the OAIC. A worrying finding is that while people now seem to have a better understanding of how ombudsmen schemes operate, a quarter (27%) does not know who to report their problems to — a significant increase on the situation six years ago (20%).

The use of personal information such as revealing one customer's data to another customer (97%), information being used for a purpose other than the reason for which it was given (97%), and being contacted by an unfamiliar organisation (96%) is considered almost universally to be inappropriate. Related to this, the backlash against unsolicited marketing activity is gaining pace, with the majority feeling annoyed (56%) with the contact or concerned about how their details were obtained by the organisation contacting them (39%). In 2013, just under half (45%) were annoyed by this activity versus just over a quarter (27%) in 2007. Australians were less likely to feel it was "a bit annoying, but mostly harmless" (11% in 2013 versus 23% in 2007).

The majority of Australians do not like their personal information being sent offshore. Eight in ten (79%) believe this to be a misuse of their personal information and nine in ten (90%) have concerns about the practice.

Australians are not keen on having their activities monitored covertly on the internet (78% are uncomfortable with this practice) and having sales and marketing approaches made to them based on their actions (69% are uncomfortable). However, they prefer this activity to the idea of having information on their behaviour stored in databases to be used to target offers at them (77% are uncomfortable).

The majority believes that most or all websites (59%) and smartphone apps (48%) collect information about the user and are uncomfortable with this practice. The result is that a growing number of people are taking pre-emptive measures to protect their information, from nine in ten (90%) refusing to provide personal information in some circumstances, to eight in ten (78%) checking the security of websites before entering personal data, to seven in ten (72%) clearing their internet browsing history, to six in ten (62%) opting not to use smartphone apps because of concerns about the way personal information would be used. Still only three in ten falsify their name (30%) or details (32%) in order to protect themselves.

The majority (60%) believes that social networking is mainly a public activity where information can be seen by many people. One in six (17%) has posted something onto a social networking site that they regret, rising to a third (33%) amongst young people.

In the face of these results it might seem strange that a slight majority (51%) continues not to read online privacy policies. The reasons that these policies are not read are concerning — it is because they are considered to be too long (52%), complex (20%) or boring (9%). The large minority (37%) reading privacy policies are rewarded by gaining the information they need to decide whether or not to use the site.

Over time this study has sought to understand the level of trust that Australians have in the way that organisations handle their personal information. It is still the case that Australians have more trust in government entities (69%) than most private enterprises, with the exception of health organisations (90%) and financial institutions (74%). Notable shifts in levels of trust since 2007 are an increase in trust in financial institutions (58% to 74%); insurance companies (46% to 54%); real estate agents (25% to 33%) and eCommerce companies (18% to 26%). The only type of company to be considered less trustworthy was market and social research organisations (35% to 30%).

The majority (60%) of Australians have decided not to deal with a private company due to concerns as to how their personal information will be used, and nearly a quarter (23%) has decided not to deal with a public organisation.

The public expects similarly high standards of transparency in data handling from all types of organisations with almost universal agreement that organisations should inform them if their personal information is lost and how they protect and handle personal information in the first place. For government agencies, nearly all Australians (96%) believe that they should tell them how their personal information is stored and protected, and that they should be informed if their personal information is lost (96%). The results for private businesses are similar (95% and 96% respectively).

Half (49%) of Australians continue to be most reluctant to provide financial details to organisations, but a small but growing proportion is reluctant to provide address (7%), date of birth (6%) or home phone number (4%) details. Nonetheless, over a quarter of the population is prepared to provide personal information in exchange for improved service (34%) or reduced prices (28%).

Reluctance to provide medical information has fallen (from 25% in 2001 to 7% in 2013). Related to this, the proportion that is prepared to have information shared is rising, with two thirds (66%) prepared to accept their doctor discussing their health information with other health professionals versus six in ten (59%) in 2007.

Australians do see circumstances in which personal liberties can be outweighed by the public good as well. In the workplace, over nine in ten Australians believe it is acceptable for employers of people: operating heavy machinery (96%); handling dangerous substances (95%); operating vehicles on company business (94%); or dealing with children and young people (91%), to undergo random drug and alcohol tests. Having said this, they expect employers engaged in these or surveillance activities to have policies in place that govern their use (85%).

Biometric data are widely available and its use concerns Australians. The majority is concerned with the need for the use of such information to access licensed premises (71%), the workplace or place of study (55%) and to do day-to-day banking (54%), but the minority (40%) is concerned with using it to get on a flight. Related to this, scanning identification documents is considered to be acceptable in order to obtain a credit card (69%), but not for more everyday activities such as purchasing general goods — even those which require the purchaser to be an adult (31%), entry to licensed premises (28%), or to purchase cigarettes (24%). Scanning identification was strongly opposed for other general goods (95% believed it is unacceptable).

Finally the survey asked Australians about their understanding of credit reporting. Half (48%) believe that they can access their information but that they may have to pay to do so, a quarter (26%) believe that their information is freely available and one in six (17%) believe that it cannot access the data at all. The balance, one in ten (9%), professes to have no knowledge on how the provisions work. One in six (17%) Australians claimed to have accessed their credit report and four in ten (43%) of these people were charged for access. Happily, in most cases (70%) the information contained in the report was correct. Almost six in ten (57%) of those people who reported incorrect information in their reports were able to have the information corrected. Nonetheless, four in ten (39%) of those with incorrect information chose not to complain. The people who did complain largely chose to do so to the organisation involved.

2.0 Background and objectives

The Office of the Australian Information Commissioner (OAIC) is an independent Australian Government agency established under the *Australian Information Commissioner Act 2010*.

The OAIC has three primary functions:

- privacy functions, conferred by the *Privacy Act 1988* (Privacy Act) and other laws
- freedom of information (FOI) functions, in particular, oversight of the operation of the *Freedom of Information Act 1982* (FOI Act) and review of decisions made by agencies and ministers under that Act
- government information policy functions, conferred on the Australian Information Commissioner under the *Australian Information Commissioner Act 2010*.

The OAIC Community Attitudes to Privacy study aims to understand Australians' changing awareness and opinions about privacy, as well as their expectations in relation to the handling of their personal information. The study also seeks views on a range of particular issues, including online privacy, credit reporting and privacy in the workplace.

The objectives of the 2013 study include:

- to assist in the OAIC's dispute resolution, regulation and strategy work, and communications work
- to provide information on privacy trends and developments for the OAIC's stakeholders
- to map changes in community attitudes since the last research and to use this information as a benchmark for future studies.

It is also worth noting that the FOI Act states that information held by the Australian Government is a national resource, and is to be managed for public purposes. In practice, this means that the OAIC is committed to making public sector information more readily and freely available to the public to maximise its reuse and value. In this regard, the OAIC will make the de-identified data available on data.gov.au, an Australian Government initiative that provides an easy way to find, access and reuse public datasets from the Australian Government.

Previous surveys

In 1990, 1991, 1993 and 1994, the Privacy Commissioner (as part of the then Human Rights and Equal Opportunity Commission) conducted surveys to measure changes in public attitudes towards and awareness of privacy-related concerns to which their activities may have contributed. Major research studies were subsequently undertaken by the former Office of the Privacy Commissioner (OPC) in 2001, 2004 and 2007, to assist the OPC to prioritise its activities based on public concerns.

The 2007 research consisted of a quantitative survey of community attitudes. A national phone survey of 1,503 adults was undertaken using Computer-Assisted Telephone Interviewing (CATI). The average time taken for the survey was 26 minutes, although it ranged up to 45 minutes.

There have been a number of significant developments in the privacy environment since the 2007 survey that shaped the current study.

The last study provided information for the then OPC to use in its submission to the Australian Law Reform Commission (ALRC) inquiry into Australian privacy law and practices.

The ALRC released its report *For Your Information: Australian privacy law and practice* (ALRC Report 108) in 2008, and the Australian Government released a response to a number of the recommendations of the report.

In November 2012, the *Privacy Amendment (Enhancing Privacy Protection) Amendment Act 2012* (Cth) was passed. This Act amends the Privacy Act to implement the major legislative elements of the Government's first stage response to the ALRC report. Key changes include a set of new harmonised privacy principles (known as the Australian Privacy Principles) that will regulate the handling of personal information by both Australian government agencies and businesses, changes to credit reporting laws, and enhanced enforcement powers for the OAIC.

Further, major changes to Federal FOI law made in 2010 established the OAIC as the body responsible for all three of these functions. The Office of the Privacy Commissioner, which was the national privacy regulator, was integrated into the OAIC at this time.

In the six years since 2007 technology, in particular, has changed. For example, in 2007 social networking site Facebook had 21 million registered members[1]. By the middle of 2013 it had over 980 million. In 2007, Twitter reported 400,000 tweets per quarter[2], by 2011 users were tweeting 140 million tweets per day[3].

The gigantic uptake of online activity has led to an age of 'big data'. Online activity, such as online shopping, has seen a sharp rise in the provision of personal information online in exchange for goods, services and other benefits.

Coupled with this is a dramatic increase in smart phone and tablet ownership and the way in which these devices are used has also changed. For example, Apple launched the first iPhone in June 2007. These devices have combined a phone with other functionality that will often rely on the provision of additional information about the user, including location information.

There have also been a number of changes in the market research industry that have shaped the approach taken to this survey. These changes include the review of the industry's privacy code, changes in telephone number sampling products and random digit dialling, changed views about the benefits of online surveys and new software and hardware enabling true multi-mode deployment of complex samples.

Clearly, these changes in technology and the public's behaviour in relation to the provision of personal information, along with business and government's ability to collect and use this information are all worthy of investigation. These themes are now woven into the study to ensure these trends can be mapped into the future.

[1] Lange, Ryan. and Lampe, Cliff. "*Feeding the Privacy Debate: An Examination of Facebook*" Paper presented at the annual meeting of the International Communication Association, TBA, Montreal, Quebec, Canada, May 22, 2008: p.20
[2] Beaumont, Claudine (February 23, 2010). "*Twitter Users Send 50 Million Tweets Per Day – Almost 600 Tweets Are Sent Every Second Through the Microblogging Site, According to Its Own Metrics*". The Daily Telegraph (London).
[3] https://blog.twitter.com/2011/numbers

3.0 Methodology

Following the 2007 study, Wallis prepared a detailed methodology report that raised a number of issues with the methodology that had been used up to that point. While it has always been difficult to interview young adults, especially those aged 18-24, because they are highly mobile, the increasing trend for this age group to use **only** mobile communications posed a problem for fixed line telephone surveying, if the views of this group were to be included at reasonable cost. In addition, the proportion of households relying solely on a fixed line phone is declining, although still around eight in ten households (80%) have a fixed line phone.

In 2007, online research was becoming increasingly popular. Online research respondents are pre-recruited and some of their characteristics are known. This made the technique particularly useful for ensuring a fast turnaround of respondents to pre-arranged specifications. Wallis suggested boosting telephone interviews with interviews conducted online, particularly for the younger age groups.

Since 2007, the approach to online research has matured. Many surveys have been conducted and providers of online surveys are now wary of over-researching younger people in their pre-recruited respondent panels. In addition, we now know that mobile young Australians are no more interested in completing surveys online than they are in talking on the telephone. In the interim, new listings of connected mobile telephone numbers have become available and it was decided to continue to interview Australians by telephone but using a mixed starting sample of fixed and mobile phone numbers.

Data collection

Data for this study was collected through Computer Assisted Telephone Interviewing (CATI) between 13 June and 10 July 2013. All calls were made from Wallis Consulting Group's CATI facility in Melbourne. In total 1,000 interviews were completed with Australians aged over 18 years of age. Quotas were set for age and location to ensure that the sample was broadly representative of the Australian population and that there were enough responses in each group of interest for robust analysis. The actual number of interviews completed by location is shown in Table 1. Table 2 shows the number of interviews conducted by age groups and Table 3 shows the number broken down by gender.

For the purpose of this report, due to rounding, percentages may not add to 100 per cent.

Table 1. Achieved responses versus population by location

Location	Base *n*	Base %	Pop. %
NSW/ACT (sub-total)	**328**	**32.8**	**33.9**
Sydney	193	19.3	20.5
Rest of NSW/ACT	135	13.5	13.3
VICTORIA (sub-total)	**263**	**26.3**	**25.1**
Melbourne	191	19.1	18.9
Rest of VIC	72	7.2	6.3
QUEENSLAND (sub-total)	**195**	**19.5**	**19.8**
Brisbane	104	10.4	9.5
Rest of QLD	91	9.1	10.3
SOUTH AUSTRALIA (sub-total)	**85**	**8.5**	**8.5**
Adelaide	56	5.6	5.8
Rest of SA /NT	29	2.9	2.6
WESTERN AUSTRALIA (sub-total)	**105**	**10.5**	**10.3**
Perth	82	8.2	8.1
Rest of WA	23	2.3	2.3
TASMANIA (sub-total)	**24**	**2.4**	**2.3**
Hobart	9	0.9	1.0
Rest of TAS	15	1.5	1.3
TOTAL	**1000**	**100.0**	**100.0**

Table 2. Achieved responses versus population by age groups

Age	Base *n*	Base %	Pop. %
18 to 24	104	10.4	12.2
25 to 34	119	11.9	17.9
35 to 54	308	30.8	36.4
55 to 64	274	27.4	15.1
65 and over	195	19.5	18.3
Total	**1000**	**100.0**	**100.0**

Table 3. Achieved responses versus population by gender

Gender	Base *n*	Base %	Pop. %
Male	432	43.2	48.8
Female	568	56.8	51.2
Total	**1000**	**100.0**	**100.0**

The interview took 26 minutes, on average, for respondents to complete. The questionnaire used for the study is available at Appendix One.

Sample — source and management

This study used a dual-frame sampling approach; that is, including both mobile and fixed line phone numbers in the starting sample. This sampling frame gives almost universal access to Australians.

One of the limitations of using mobile phone sampling is that it is not possible to determine the location of the telephone's owner, which is important for the study given the critical importance that respondents are not called at inappropriate times as well as the logistics of filling location-based quotas. For this reason, and partly to keep the project within budget, the proportion of mobile phone numbers was lower than fixed line numbers.

To accommodate the dual-frame approach, the sample included Random Digit Dialling (RDD) mobile and fixed line numbers generated by SampleWorx, as well as additional sample of fixed line telephone numbers provided by SamplePages. Both sample sources are only available for the purposes of market and social research.

The decision to use RDD mobile and fixed line numbers as the primary source for the sample was made to ensure that the respondent base was as free from bias as possible. The RDD process takes known number ranges for Australian fixed line and telephone numbers and generates phone numbers in those ranges randomly. For mobile RDD, these numbers are verified as "live" by the sample provider prior to inclusion in the sample.

The inclusion of a mobile sample facilitated the sending of SMS messages to sample members. After they had been called once with no contact made, 4,411 sample members were sent an SMS with the following wording:

> *We are contacting you on behalf of the Office of the Australian Information Commissioner to do a survey on privacy. Wallis market and social research will call you from 03 9940 2###. You do not have to do the survey. When we call, let us know and we will not call again. More info: www.oaic.gov.au or www.wallisgroup.com.au.*

They were able to reply to the message to opt out of the study. In total 96 replied with 85 opting out of the study.

The standard ring time for the project was increased to 30 seconds to allow sufficient time for sample members with mobile phones to locate the phone and answer it.

Questionnaire development

The questionnaire was based on the last Community Attitudes to Privacy Study conducted in 2007. The questionnaire was developed for the 2013 study by the OAIC in consultation with an internal steering committee comprised of representatives from the OAIC's three branches — Dispute resolution, Regulation and strategy and Corporate support and communications.

The Privacy Advisory Committee — a Committee established under the Privacy Act and comprising of representatives from unions, health service providers, business and government as well as a consumer representative — was also consulted. The study's primary sponsor, the Commonwealth Bank of Australia, was provided with an opportunity to contribute a question to the survey. The

Commonwealth Bank provided feedback on a number of areas covered by the survey but did not seek the addition of a question.

A number of questions were retained in the form that they had been asked since the study was first conducted in 2001. These questions relate to awareness of privacy laws and trust in organisations.

Most other questions were modified slightly to reflect changes that have occurred. For example the last study contained a set of questions on attitudes towards CCTV, which was a big issue in 2007. Similarly, a question on trustworthiness of industry sectors was modified to include social media and technology companies, which were in their infancy then.

Some new questions were added, including questions on what people regard as the biggest privacy risks, transparency of information handling practices, data loss, online tracking, smart phones, social networking, the actions people take to protect their own privacy, and credit reporting.

It was also decided to define the scope for the study at the beginning of the questionnaire by providing the following information:

In Australia, privacy law relates to the protection of an individual's 'personal information'. This is any information about you that identifies you or could reasonably be used to identify you. For example, this includes things like:

- *your name or address*
- *financial details*
- *photos*
- *your opinions and beliefs*
- *membership of groups and affiliations*
- *racial or ethnic origin*
- *health information (including genetic information)*
- *sexual preferences*
- *criminal record.*

Pilot study

A pilot study comprising 21 interviews was conducted on 6 June 2013. The pilot aimed to test the questionnaire for sense and duration. While the questionnaire was deemed by the pilot team to have good flow and was well understood by respondents, it ran for 28 minutes. Following the pilot the questionnaire was modified slightly to reduce the overall length. The main method used to do this was to assess each question and to combine together some that were measuring very similar ideas. Nonetheless, nearly all questions were deemed to be essential to the study and the average length was only shortened by two minutes.

Weighting

The data were weighted for age, sex and location to adjust it to represent the Australian community. As interviewing quotas had been set for age and location to reflect the actual numbers in the population, the effect of the weighting was minimal.

Weighting has the effect of altering the number of responses that should be considered when statistical analysis and testing are carried out on the results. This is because, while weighting makes the total number of interviews represent the population of interest, in this case the Australian community, it has not changed the actual number of interviews conducted and the relative differences in the sizes of those groups. It is this base that significance tests use to show whether or not results are really different from each other, and therefore worthy of comment, or whether they relate to sample design.

Table 4. Weighting and sample variance

Demographic Category	Base (#)	Base (#)	Target weight (#)	Weighted (#)	Difference (Base % vs Weighted %)	Effective Base	Sample variance for survey estimates of 10%-50%
Age							
18-24 years	104	10%	2,013,963	12%	-2%	102	±6-10%
25-34 years	119	12%	2,956,390	18%	-6%	116	±5-9%
35-54 years	308	31%	5,999,382	36%	-6%	302	±3-6%
55-64 years	274	27%	2,495,351	15%	12%	269	±4-6%
65 years and over	195	20%	3,006,728	18%	1%	191	±4-7%
Region							
Greater Sydney	193	19%	3,384,255	21%	-1%	193	±4-7%
Rest of NSW/ACT	135	14%	2,198,103	13%	0%	135	±5-8%
Greater Melbourne	191	19%	3,112,669	19%	0%	191	±4-7%
Rest of Vic.	72	7%	1,029,614	6%	1%	72	±7-12%
Greater Brisbane	104	10%	1,567,604	10%	1%	104	±6-10%
Rest of Qld	91	9%	1,699,591	10%	-1%	91	±6-10%
Greater Adelaide	56	6%	961,565	6%	0%	56	±8-13%
Rest of SA/NT	29	3%	435,463	3%	0%	29	±11-18%
Greater Perth	82	8%	1,326,617	8%	0%	82	±6-11%
Rest of WA	23	2%	376,077	2%	0%	23	±12-20%
Greater Hobart	9	1%	163,567	1%	0%	9	±20-33%
Rest of Tas.	15	2%	216,689	1%	0%	15	±15-25%
Gender							
Male	432	43%	8,043,672	49%	-6%	390	±3-5%
Female	568	57%	8,428,142	51%	6%	512	±3-4%
Total	**1000**	**100%**	**16,471,814**	**100%**	**0%**	**891**	**±2-3%**

In survey research it is usually impossible to talk with everyone to be certain about how the community feels about an issue. Instead researchers talk to smaller groups of people, or a sample, and estimate what everyone thinks on the basis of the answers from the people they have spoken with. In this case, 1000 people were interviewed.

People in the sample are chosen to represent the community and, as explained earlier, minimum numbers of people are required to make reliable estimates. Nonetheless, it is impossible to be completely certain that a sample of respondents thinks exactly the same way as everyone making up the population. There are, therefore some errors inherent in making an estimate from a smaller group of the population. In addition, there is an issue of variability. Every time a survey is conducted there is a likelihood that the survey results may differ slightly as the same people are not being interviewed. Quite small total numbers of interviews may, nonetheless, give very accurate estimates. The total sample of 1,000 gives answers that will fall within a 2-3% error range, the bulk of the time.

Researchers run "significance" tests to check if differences between two results are real or whether they have happened because of variability. The standard approach is to report on findings at the 95% level. This means that if the survey is repeated 100 times, 95 times out of 100 times, the results would be within the same error range. Table 4 shows the error limits for variables that are used in analysis. Thus, readers can be confident that all results reported are based on findings that are real and different by at least the amounts shown in the table, which for age is 3-10%, depending on age group, and for gender is 3-5%.

The sample variance is at its greatest the closer to 50% the results are and at its least the closer to 0% or 100%. Table 4 shows the accuracy of survey estimates for the analytical variables for 10% and 50% — most answers will fall somewhere between these two, but significance tests calculate the actual value for every number.

Analysis

The data from this study and the 2007 study were cross-tabulated and significance tests were run on the data at the 95% confidence interval as outlined earlier. Cross-tabulation involves automatically adding up all the responses to a question by some variables that are of interest, for example, age, gender or location. The analyst can then see patterns of response and whether there are any different responses between variables, and whether variables are dependent on others. For example, there is a clear relationship between increasing level of education achieved and increasing household income.

Definitions

Most definitions used are self-explanatory, for example, age groups, geographic location and gender. Throughout this report people working in different types of occupations are referred to as "blue collar" and "white collar". These are standard classifications used by the Australian Bureau of Statistics and follow the Australia and New Zealand Standard Classification of Occupations (ANZSCO). White collar refers to people working in largely office based roles and includes Managers, Professionals, Community and Personal Service Workers, Clerical and Administrative Workers, and Sales Workers. Blue collar refers to people working in mainly manual occupations and includes Technicians and Trades Workers, Machinery Operators and Drivers, and Labourers. These groups are divided into upper and lower. For white collar workers "upper" generally denotes managers or professionals while lower refers to more clerical positions. For blue collar workers "upper" generally denotes skilled trades people while "lower" refers to unskilled workers.

4.0 Detailed findings

This study of community attitudes to privacy covered a number of key areas, namely:

- awareness of Federal privacy laws
- general attitudes towards privacy and personal information
- privacy problems and complaints
- trust
- personal responsibility
- medical and health information
- privacy in the workplace
- ID scanning
- internet and smart phones
- ID theft and fraud
- credit reporting.

The survey findings are organised under these key headings. The questionnaire, which is appended, does not follow this same structure exactly as it was more important to ensure that questions flowed logically for the respondent than for the analyst.

Definition of 'personal information'

In Australia, privacy law relates to the protection of an individual's personal information. Therefore, a number of survey questions refer to 'personal information'. As this was a lengthy survey, the decision was taken to provide respondents a definition of what is meant by personal information based on the definition in the Privacy Act.

In Australia, privacy law relates to the protection of an individual's 'personal information'. This is any information about you that identifies you or could reasonably be used to identify you. For example, this includes things like:

- *your name or address*
- *financial details*
- *photos*
- *your opinions and beliefs*
- *membership of groups and affiliations*
- *racial or ethnic origin*
- *health information (including genetic information)*
- *sexual preferences*
- *criminal record.*

In previous studies, while the line of questioning aimed to keep respondents focussed on the area of interest, some of the answers showed that they were straying into the area of personal space in their answers.

Giving survey participants a working definition early in the survey does not seem to have had a major impact on answers to questions that have been asked before. It has, naturally, affected the range of answers given to open-ended questions, particularly those at the beginning of the survey where participants were asked to define perceived privacy risks and areas of perceived infringement of their privacy.

Factors that may have influenced responses

Not surprisingly privacy has rarely been out of the news since the study was last conducted in 2007. The media continues to report on exciting new technologies that raise privacy questions, as well as significant invasions of privacy and data breaches.

Not long before the study commenced the media started to report on US intelligence surveillance programs that involved the participation of technology companies that offer a range of popular online services. Public debate on these revelations grew significantly during the life of the survey and may have had some effect on how people chose to respond to some of the survey questions, in particular questions on general attitudes to privacy, trust and the internet.

Awareness of Federal privacy laws

The Privacy Act is an Australian law that regulates the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information.

The Privacy Act is of pivotal importance to this study.[4] One of the key reasons for undertaking this study now is to gain a baseline measure of understanding prior to introduction of amendments to the Privacy Act in March 2014. Nonetheless, the name of the legislation will remain the same.

Chart 1 shows that the vast majority (82%) of Australians claimed to be aware of Federal privacy laws prior to this interview. The proportion of respondents who reported they were not aware was one in six (17%) and a very small proportion (1%) of respondents indicated they were unsure.

This compares favourably to the result when last measured when two thirds of Australians claimed awareness of the laws (69%). It continues a gradual increase in awareness from its low point when first measured in 2001 at just over four in ten (43%) to a majority awareness in 2004 of six in ten (60%).

The pattern of awareness has not changed substantially. In 2013, awareness peaks in the 35-64 age range at just under nine in ten (86%). This is similar to 2007 where awareness was also relatively high amongst this age group (74%), compared to younger and older Australians.

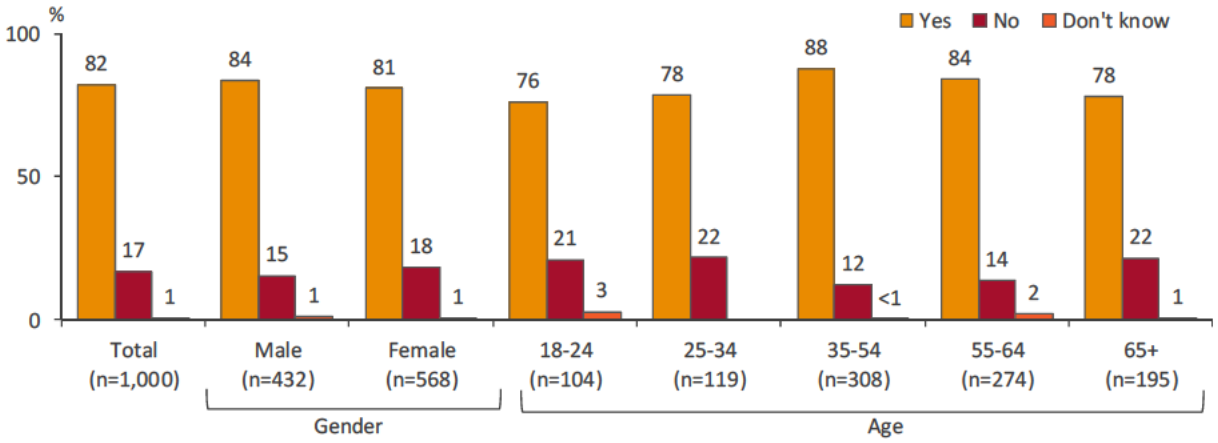
Australians maintain a similar level of awareness of Federal privacy laws regardless of gender. In 2013, just over eight in ten males (84%) and females (81%) were aware of Federal privacy laws versus seven in ten of each in 2007 (70% and 68% respectively).

The level of awareness increases in accordance with educational attainment, and is significantly greater amongst those who have completed year 12 than those who have not. In 2013, seven in ten (72%) respondents who completed up to year 10 were aware of Federal privacy laws, compared to

[4] See: http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act

around eight in ten of those who have completed year 12 (81%), a Diploma/TAFE (82%) or a Bachelor's degree (85%) and is at nine in ten (91%) amongst those with a Postgraduate degree.

Chart 1. Awareness of Federal privacy law by age



Base: All respondents

Q6 Were you aware of the Federal privacy laws before this interview?

General attitudes towards privacy and personal information

Biggest privacy risk

Survey participants were asked at the outset of the survey interview to name the biggest privacy risks that they think face the community. Nearly half of the population (48%) suggested that using online services and social media sites pose the greatest risk. As can be seen in Table 5, this is by far the biggest risk perceived by six in ten respondents aged 18-24 years (60%). Australians working in white collar jobs are the most concerned about this risk.

ID fraud and theft (23%), and the related problems of fraudulent use of financial information (11%), and easy access to personal details (9%) was considered to be the second biggest issue. People aged between 25 and 45 were the most concerned about this. This may be because people in this age group are also the most likely to have been the victim of this activity, or to know someone who has been (see 'ID theft and fraud', below)'. Residents of Queensland (28%) and Western Australia (29%) continued to be more concerned about this issue than other Australians. As was the case in the 2007 study, residents of Western Australia reported higher levels of ID fraud and theft. People aged 55–64, while still concerned about ID fraud and theft, reported the highest levels of concern about fraudulent use of financial details rather than other personal details. Again this seems to relate to personal experience. There was general unease about the lack of security of personal information, which peaked at one in eight people aged 25–34 (13%).

As noted above, during the interviewing period there was global public debate around US surveillance programs such as PRISM which may have led to data security and breaches being considered the third greatest risk, mentioned by one in six (16%) Australians.

Other issues were identified as the biggest privacy risk by less than one in twenty Australians overall, although there were some differences by respondent type. For example, different age groups gave greater importance to some of these risks:

- amongst 25–34 year olds smartphone apps were considered a problem (7%)
- the gathering of profiling information for marketing or commercial purposes was mentioned by more than one in twenty people aged 35–54 (7%)
- people aged over 50 felt more threatened by unsolicited phone calls (5%) than younger Australians
- over one in ten younger adults (11% of 18–24 year olds) could not think of any privacy risks.

Some other points of interest are:

- Only people working in lower white or blue collar occupations felt that information relating to ethnicity or race poses a privacy risk, with the greatest concern being amongst people in lower blue collar occupations (3%).
- Men were significantly more likely than women to worry about information being captured and handled by the government (5% compared with 2%).
- Residents of South Australia, Western Australia and the Northern Territory were the most concerned about organisations collecting profiling information for commercial gain (9%).

Table 5. Biggest privacy risks facing people today by age

Q1. What do you think are the biggest privacy risks that face people today?	Age					
	18-24 (n=104) %	25-34 (n=119) %	35-54 (n=308) %	55-64 (n=274) %	65+ (n=195) %	Total (n=1,000) %
Online services/ social media sites	**60**	49	**50**	46	38	48
ID theft/ fraud	18	**28**	**26**	23	17	23
Data security/ data breaches	13	13	19	16	18	16
Credit reporting	-	-	**2**	**2**	**3**	2
Smart phones/ apps	2	**7**	3	2	3	4
Unsolicited phone calls	-	2	3	**5**	**5**	3
Surveillance	4	5	3	2	2	3
ID scanning	-	-	1	**2**	1	1
Sending information overseas	-	1	1	1	2	1
Workplace privacy	1	-	1	-	-	1
Personal details too easily available/accessible/not secure	9	**13**	6	**12**	10	9
Information relating to ethnicity/ race	1	1	1	-	1	1
Unauthorized monitoring of information/data mining	3	1	1	2	2	1
Financial details/ information/ fraud	8	9	10	**18**	13	11
Commercial interests/ marketing about buying habits/ profile	1	3	**6**	3	2	4
Government information sharing/ information collection	2	3	3	5	5	3
Information relating to religious beliefs	-	-	-	1	1	<1
Criminal history too easy to access	-	-	-	-	1	<1
How frequently we have to give out personal information	-	-	<1	-	1	<1
Other	-	2	2	3	3	2
Don't know	**11**	7	5	5	9	7

Base: All respondents
Note: Bold denotes a significant increase

Table 5 shows these results in more detail by age group, as this was the biggest differentiating factor in views.

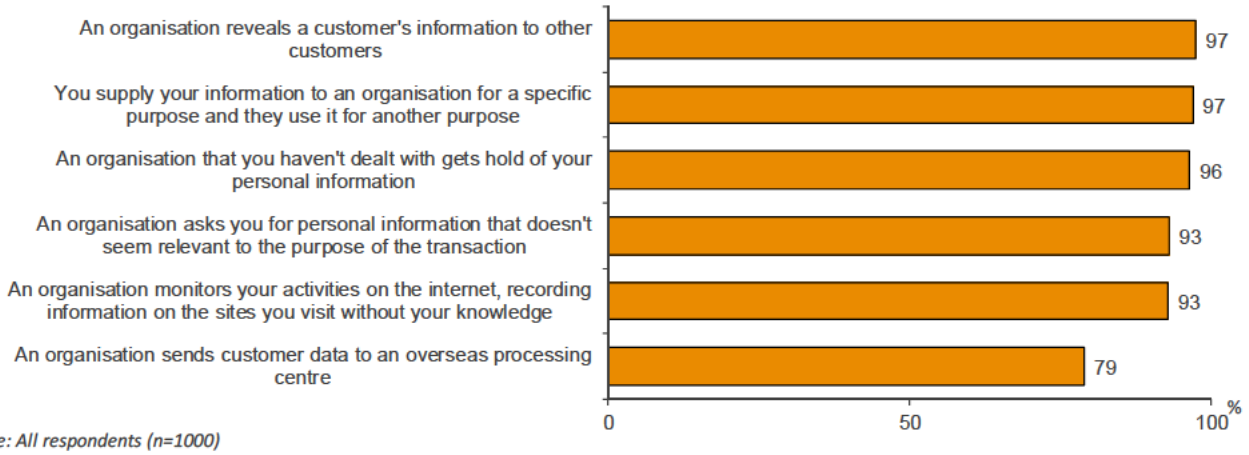
Generally, Australians held very consistent opinions. However, some significant differences in results are summarised below.

- ID fraud and theft was of greatest concern to people aged between 25 and 54 years of age.
- Inappropriate access to financial details was of most concern to people aged between 55 and 64.
- Lack of security of personal details was of greatest concern to people aged 25–34 and 55–64.
- Potential risks posed by smartphone apps caused more than one in twenty people (7%) aged 25–34 to mention this as a privacy risk spontaneously — twice the level of any other age group.
- Unsolicited phone calls were of greatest concern with people aged over 55.
- Credit reporting was mentioned increasingly by people aged over 35.
- ID scanning was more of a concern for 55–64 year olds.
- People aged under 24 were the most likely to not hold any fears with one in ten (11%) being unable to identify any risks.

Activities considered a misuse of information

Australians were read a number of scenarios similar to some that had been put to them in a previous study in 2007. They were asked whether or not they considered each scenario to describe misuse of personal information. The majority agreed that all scenarios represented a misuse of information.

Chart 2. A misuse of information



Base: All respondents (n=1000)

Q12 Which of the following instances would you regard to be a misuse of your personal information?

There is almost universal agreement that the following are a misuse of personal information.

- Revealing personal information to other customers (97%);
- Using personal information for a purpose other than the one it was provided (97%); and
- The collection of personal information by an organisation that a person has not dealt with before (96%).

More than nine in ten (93%) people believe that an organisation asking for information that is not relevant to the transaction and monitoring activities on the internet without the individual's knowledge are misuses too. Almost eight in ten (79%) believe sending customer data to an overseas processing centre is also a misuse.

Similar scenarios were asked in 2007 and these results are similar with the 2013 results. Over seven in ten respondents reported it is a misuse of their personal information for each scenario.

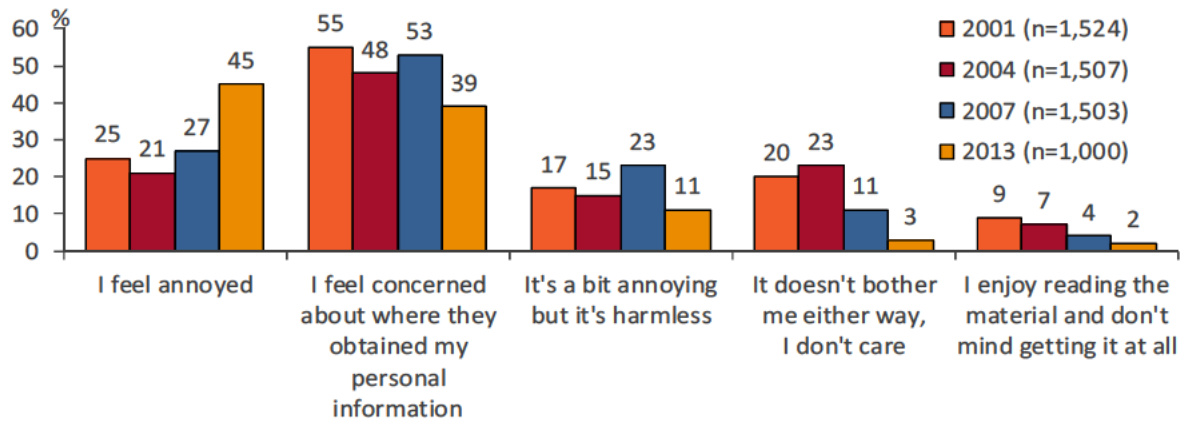
In 2007, the scenarios were asked for private business and government departments separately. The results were as follows:

- A (business / government department) monitors your activities on the Internet, recording information on the sites you visit without your knowledge (96% / 86% respectively)
- A (business / government department) asks you for personal information that doesn't seem to be relevant to the purpose of the transaction (94% / 87% respectively)
- You supply your information to a (business / government department) for a specific purpose and the business/agency uses it for another purpose (94% / 86% respectively)
- A (business / government department) you haven't dealt with gets hold of your personal information (93% / 73% respectively).

Australians have been asked how they feel when an organisation they have not dealt with sends them unsolicited marketing information. It appears that Australians are feeling increasingly annoyed by this practice, with the proportion of people who say it annoys them reaching almost half of the population (45%) from a quarter when it was first measured in 2001 (25%).

The other options, namely it is annoying but harmless (11%) declined by half compared with the last survey in 2007. Only one in twenty Australians now say that unsolicited marketing information either doesn't bother them (3%) or that they enjoy reading it (2%). Together these categories accounted for three in ten Australians when measured in 2001 and 2004.

Chart 3. Feelings in relation to being sent unsolicited marketing information by an unknown organisation



Base: All respondents

Q33 Which of the following statements best describes how you generally feel when organisations that you have never dealt with before send you unsolicited marketing information?

The level of concern with how their personal information was obtained seems to have decreased since 2007, however, it is worth noting that when last asked, this question allowed multiple responses. Therefore the decline from a situation where just over five in ten (53%) respondents were concerned in 2007, to just under four in ten in 2013 (39%) may relate to the fact that respondents had to choose one of the options presented to them, not many.

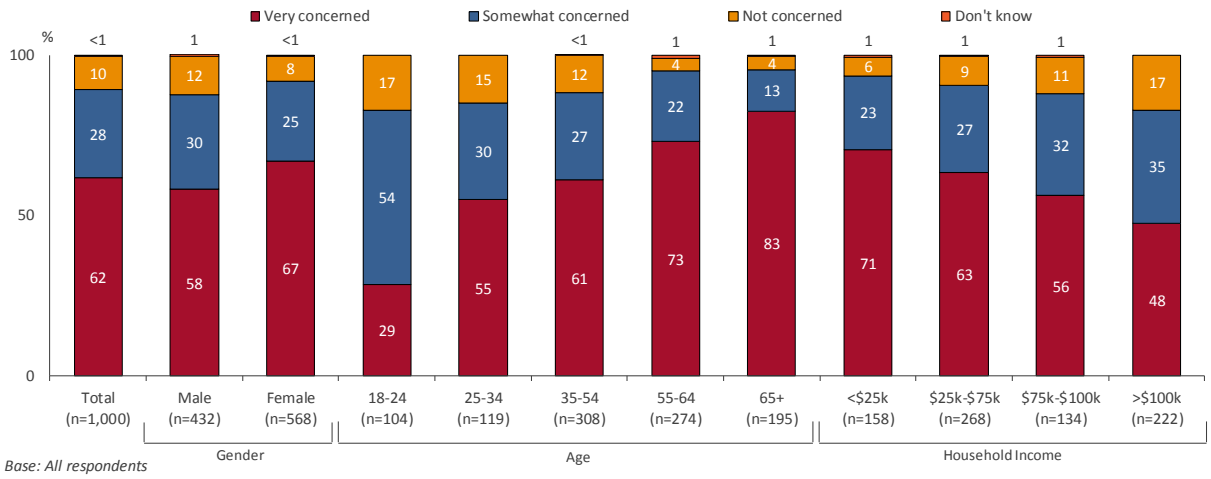
Concern about sending personal information overseas

When asked to express their level of concern over Australian organisations sending customers' personal data overseas, six in ten (62%) expressed strong concern (in 2007, 63%) with a further three in ten (28%) saying they were somewhat concerned about this practice (in 2007, 27%).

While the results are similar in comparison to 2007, there were some notable differences amongst respondents, particularly:

- Older people were more concerned than younger people. While eight in ten (83%) people aged 18–24 were concerned, the proportion who were very concerned (29%) was considerably lower than amongst people aged over 65. Nearly all (96%) people over 65 were concerned, with eight in ten (83%) of them being very concerned.
- High income households were less concerned than lower income households. Nine in ten (94%) people in low income households were concerned with the majority (71%) being very concerned. Amongst people living in households with incomes above $100,000 eight in ten (83%) people were concerned with just under a half (48%) being very concerned.
- Women were more concerned than men. In particular, two thirds of women (67%) were very concerned out of a total of nine in ten (92%) being concerned, compared with six in ten (58%) men being very concerned out of a total of nine in ten (88%) being concerned.

Chart 4. Concern about personal information being sent overseas



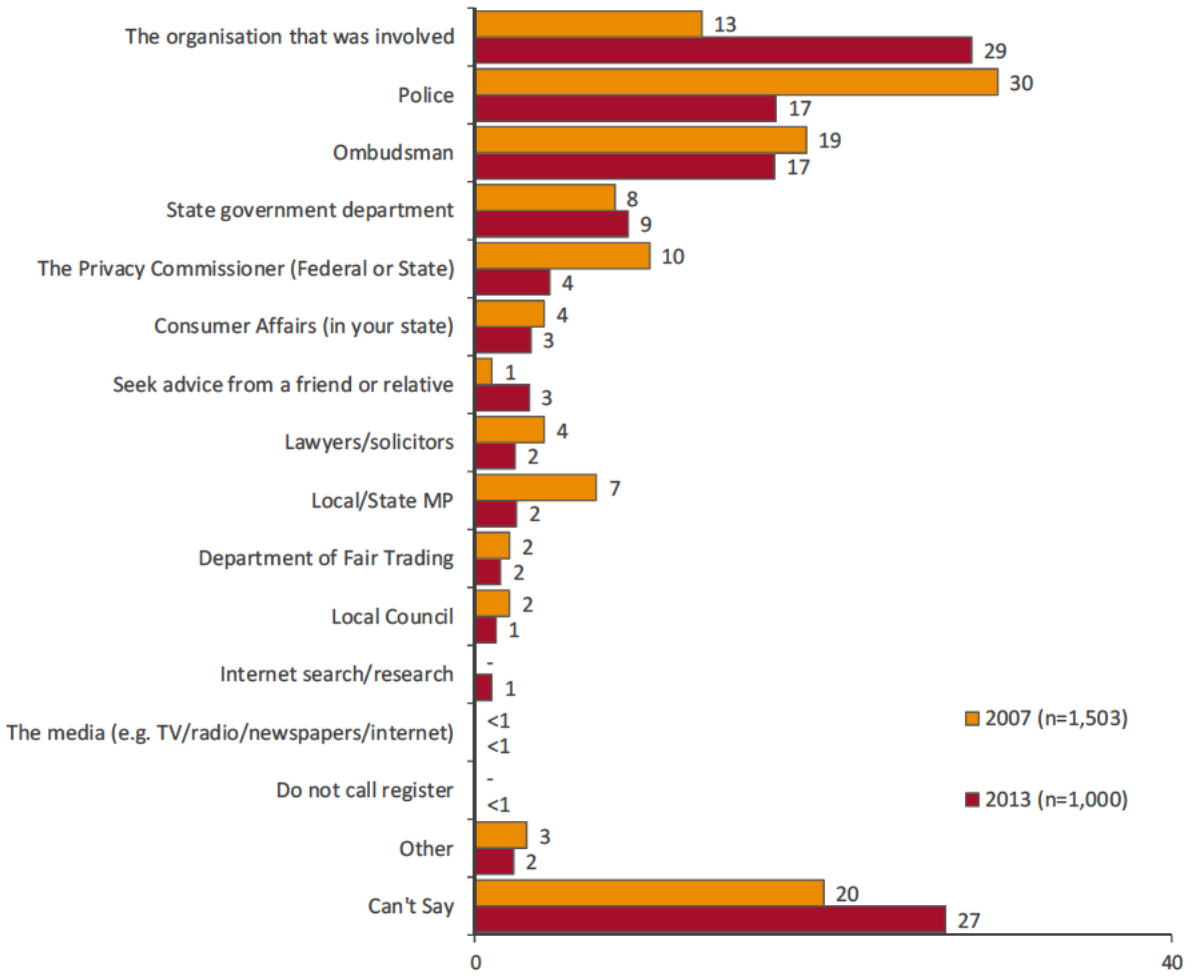
Q13 How concerned are you about Australian businesses sending their customers' personal information overseas to be processed?

Privacy problems and complaints

Respondents were asked whether they had experienced a problem with how their personal information had been handled in the last 12 months. This question has not been asked before and demonstrates that a considerable proportion of the community had experienced problems.

A third (33%) of Australians said that they had a problem with the way their personal information was handled in the last year. The proportion rises steeply amongst working Australians (38% of those working versus 26% of those not working). It increases steeply as household income rises to the point where nearly four in ten Australians (39%) living in households earning over $100,000 have had a recent problem.

Chart 5. Organisations people would report misuse of personal information to



Base: All respondents

Q17 If you wanted to report misuse of your personal information to someone, who would you be MOST likely to contact?

In previous studies, people had been asked to comment on the organisations they believe are appropriate to report such a misuse to. Chart 5 shows 2013 responses compared to 2007:

- More people are now aware that they should contact the organisation that misused the information. Three in ten (30%) suggest this is the best course of action (versus 13% in 2007).

- Fewer people suggested that reporting such information to the Police would be appropriate, with the proportion dropping to one in six (17%) from three in ten (30%).
- A similar proportion thought that they would go to the appropriate Ombudsman (17%) or government department (9%) as when last measured (19% and 8% respectively in 2007).
- The proportion who mentioned the Privacy Commissioner (4%) declined from 2007 (10%).
- There was an increase in the proportion of people who did not know who to report problems to — now over a quarter (27%) of the population gave this response —up from one in five (20%). These respondents were also less likely to be aware of privacy laws (34%) in comparison to those who were aware (25%).

Trust

This section examines the extent to which people's level of trust in certain organisations has a bearing on the amount and nature of information they are willing to provide. Topics examined are:

- the types of information that people are reluctant to provide
- the levels of trust that people place in different types of organisations' information handling capabilities
- expectations of transparency in information handling practices in both the public and private sectors (including when it comes to data breach)
- attitudes towards providing personal information in exchange for benefits.

Types of personal information people are reluctant to provide

People continue to be the most concerned about providing financial details (58%) and the proportion of people who display this level of concern has been constant since it was first measured in 2001 (59%). While the provision of this information is a concern for all, reluctance to provide these details increases with age, with under a half of people aged 18–24 mentioning it (44%) compared with six in ten amongst people aged 65 or over (60%).

After financial details, there have been some changes — some of which can be explained by the provision of the definition of 'personal information' at the beginning of the questionnaire. In particular, mentioning 'photographs' and 'sexual preferences' in the introduction has clearly raised awareness of the sensitivity of these types of personal information and they have been mentioned spontaneously for the first time (7% and 3% respectively).

The changing technological environment has undoubtedly underpinned other trends. For example, 'home address', is becoming a more protected piece of information with a quarter of people saying they are reluctant to give this (24%) in comparison to almost one in five people (19%) in 2007. This result is strongly related to age, with almost twice as many people aged under 35 (32%) being reluctant to provide this information compared to people aged 55–64 (15%) or 65 and over (17%). Victorians are also the least reluctant to give this information (29%).

Other interesting trends are:

- An increased reluctance to provide date of birth details, particularly amongst people who are working, in general, and those who are earning high incomes in particular.

- Reluctance to give a phone number has declined since 2007. Queenslanders are the least concerned with giving out their phone numbers (7%). Women are significantly more reluctant (17%) than men (12%) to give this information.
- An increasing proportion of Australians feeling reluctant to discuss the composition of their households (from 1% in 2001 to 6% in 2013), although there has also been a drop in the proportion of people reluctant to divulge their marital status (from 7% in 2007 to 3% in 2013). Taken together these items have remained consistent, so this may reflect changes in living arrangements in general.
- There has been a continuous decline in concerns over providing genetic information. The proportion of people who are reluctant to provide generic information since it was first measured in 2001 has decreased from over one in ten people (13%) to less than one in ten people (1%) in 2013.

Table 6. Information Australians are reluctant to provide to businesses and Government

Q2. In general, what types of information are you reluctant to provide?	2001 (n=1,524) %	2004 (n=1,507) %	2007 (n=1,503) %	2013 (n=1,000) %
Financial details	59	58	*43*	58
(Home) Address	14	20	19	24
Date of birth	7	8	**10**	16
(Home) Phone number	17	22	**25**	15
Name	6	7	*4*	10
Email address	11	19	*14*	7
Medical information	25	21	*6*	7
Photo ID/ information/ passport / driver's licence number/ cards and access numbers	-	-	-	7
Household composition and relationships	1	2	**4**	6
Religion/ Personal Beliefs/ Affiliations	2	3	2	4
Marital status	9	9	*7*	3
Sexual preferences	-	-	-	3
Genetic information	13	11	5	1
Other	-	-	4	4
None	16	11	10	9

Base: All respondents
Note: Bold denotes a significant move up between 2004 to 2007; Italics denotes a significant shift down between 2004 to 2007
Note: Answers add up to more than 100 as multiple responses were given

When asked which one of these pieces of information they were **most** reluctant to provide, financial information was by far the most often mentioned (49%) and all other items shown in Table 7 were mentioned by fewer than one in ten people, namely address (home and email), date of birth, phone number, medical or genetic information and the composition of the household.

The reasons for this reluctance are shown in Table 8. Some interesting trends emerge here. Firstly, the proportion of Australians who simply stated that they were reluctant to give information because 'it's none of their business' has halved over the last 12 years from a half of the population in 2001 (51%) to a quarter (25%) now. At the same time security concerns (19%) and the potential for personal financial loss (15%) have risen significantly (from 2% and 7% respectively in 2001).

Table 7. Piece of information Australians are most reluctant to provide

Q3. Which one of these [answers given for Q2] do you feel MOST RELUCTANT to provide?	2001 (n=1,524) %	2004 (n=1,507) %	2007 (n=1,503) %	2013 (n=1,000) %
Financial details / Income	51	51	*53*	49
(Home) Address	4	7	7	7
Date of birth	1	1	**3**	6
(Home) Phone number	3	5	**9**	4
Email address	2	5	5	2
Medical information	7	5	*2*	2
Household composition and relationships	<1	<1	**2**	2
Genetic information	3	2	*<1*	<1

Base: All respondents
Note: Bold denotes a significant move up between 2004 to 2007; Italics denotes a significant shift down between 2004 to 2007

Table 8. Reasons for reluctance to give key piece of information

Q4. What is your MAIN reason for not wanting to provide [answer from Q3]?	2001 (n=1,524) %	2004 (n=1,507) %	2007 (n=1,503) %	2013 (n=859) %
It's none of their business/ privacy	51	44	*36*	25
For safety/ security/ protection from crime	2	6	**12**	19
May lead to financial loss/ people might access bank account	7	8	**14**	15
The information may be misused/ information might be passed on without my knowledge	12	8	**11**	12
Unnecessary/ irrelevant to their business or cause	2	5	**9**	8
I do not want to be identified	3	1	**2**	6
I do not want people knowing where I live or how to contact me	6	5	5	5
I don't want to be bothered/ hassled/ hounded by phone or door to door	1	5	**12**	4
Don't want junk mail/ unsolicited mail/ SPAM	1	5	**11**	2
Discrimination	4	3	*2*	2
Other	3	3	*2*	2
Can't say	4	2	*1*	-

Base: All giving one item of personal information that they would feel reluctant providing
Note: Bold denotes a significant move up between 2004 to 2007; Italics denotes a significant shift down between 2004 to 2007

Reluctance to provide information for fear of the sales and marketing repercussions peaked in 2007. At that time nearly a quarter of the population said either that they were reluctant to give information for fear of being hounded by tele or door to door sales people (12%) or the fear that it would lead to unwanted mail (11%).

In the 2013 study, just over one in twenty Australians reported that they have these concerns (4% and 2% respectively). These trends may also relate to the introduction of the *Spam Act 2003* and the *Do Not Call Register Act 2006*. Both pieces of legislation clarified Australians' rights and provided an avenue for complaint.

Providing personal information for benefits

Participants were asked whether discounted purchases, a prize or improved service would overcome this reticence. As Chart 6 shows, the majority says that they are not prepared to exchange personal information for these benefits. However, a sizeable minority says they are likely to give information in exchange for a tangible benefit, particularly in exchange for lower prices (28%) or better service (34%).

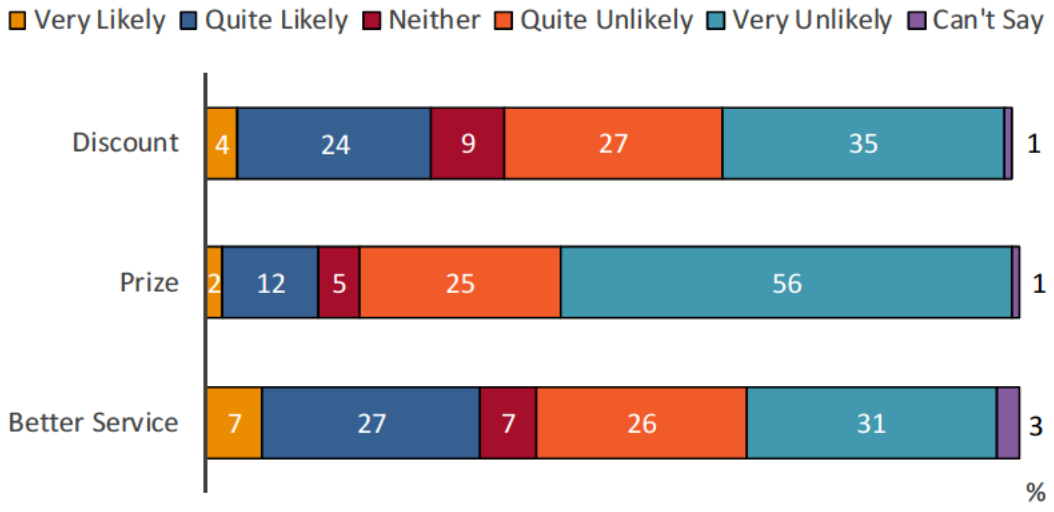
Respondents in 2007 were asked whether they are likely to give up information in exchange for a lower prices or a prize. Just over two out of ten (22%) respondents said they would in exchange for a discount (22%) and over two in twenty (13%) said they would for a prize.

Prizes are considered to provide the least incentive for giving personal information with over eight in ten people (81%) saying they are unlikely to do this, with well over half of the population (56%) saying that they are very unlikely to do so.

Respondents were more willing to provide personal information in exchange for better services if they are aged 18-24 (41% compared with 29% for people aged over 35) or if they live in a metropolitan area (37% compared with 28% in regional Australia).

People who are not working and/or live in households that earn less than $75,000 are the least likely to trade off personal information for better service.

Chart 6. Australians' willingness to give personal information in exchange for a benefit



Q9/10/11 *How likely or unlikely are you to provide your personal information to an organisation if it meant you would receive discounted purchases/the chance to win a prize/better service?*

Transparency of information handling practices in public and private sectors

Australians have generally demonstrated a higher level of trust in the public sector than in private organisations. They were asked a new series of questions designed to ascertain if there is a difference in expectations in regards to the transparency of information handling practices of public and private sector organisations.

Australians' answers suggest that while they believe government agencies should be transparent in the handling of their information, they are more demanding of being informed if that information is mishandled (96% agree with both these propositions, and 78% and 88% respectively strongly agree). The results were similar for the private sector (95% and 96%), although the increased importance of being informed in the event they lose personal information over being transparent in the manner information is to be used was less marked (with 81% and 85% respectively agreeing strongly with these propositions).

Australians hold clear views on the way in which private and public sector organisations should handle their information, with fewer than one per cent being unable to offer their opinions.

Table 9. Transparency of information handling practices in public and private sectors

Q14 items	Strongly Agree %	Somewhat Agree %	Neither %	Somewhat Disagree %	Strongly Disagree %	Don't Know %
It's extremely important that government agencies tell me how they protect and handle my personal information	78	18	**2**	2	1	0
It's extremely important that private sector organisations tell me how they protect and handle my personal information	81	14	1	3	1	0
If a business loses my personal information they should tell me	85	11	1	2	1	1
If a government agency loses my personal information they should tell me	88	8	1	1	1	0

Q14 Thinking about the way that your personal information is handled by private sector and organisations and government agencies, do you agree or disagree with the following statements?

Level of trust in types of organisations

Australians were asked to state the extent to which they trust twelve different types of organisation. Health service providers continue to enjoy the highest levels of trust with nine in ten (90%) Australians saying they are trustworthy — the same level (91%) as when measured six years ago. Social media organisations were considered to be the least trustworthy with only one in ten (9%) respondents trusting them with their personal information.

Of the types of organisations that were included in the 2007 study, four have greater levels of public trust in them:

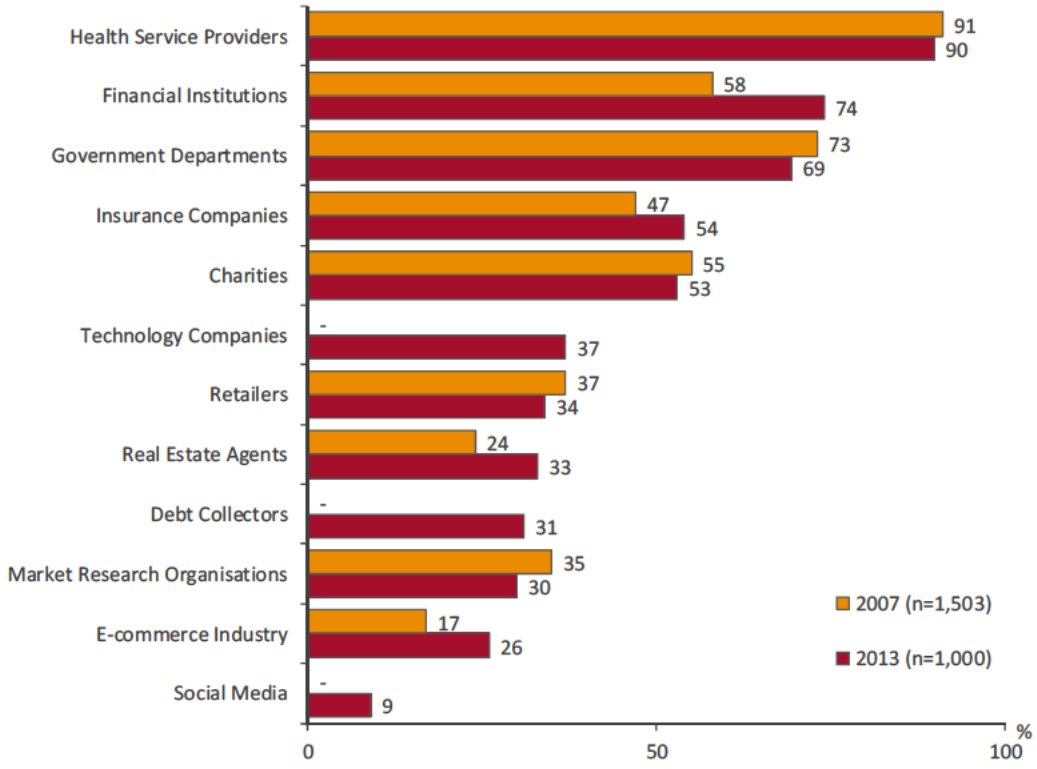
- Financial institutions enjoy trust amongst three quarters of the public (74%) compared with six in ten in 2007 (58%).
- Insurance companies have moved up 9 percentage points (from 46% to 54%).

- Real estate agents are now considered trustworthy by a third of the population (33%) compared with a quarter six years ago (24%).
- e-Commerce companies now have the trust of a quarter of the population (26%) compared with one in five (18%).

The position of health service providers, government departments, charities and retailers were relatively unchanged. The most trusted organisation to handle personal information is health service providers (in 2013, 90%; in 2007, 91%). The level of trust associated with government departments has slightly decreased (in 2013 to 69% from 73% in 2007). Charities remain relatively consistent as just over half of the respondents (53% and 55%, respectively) reported they trust charities to handle personal information. Just over one in three respondents reported they trust retailers (34% and 36%, respectively).

Only market and social research companies were considered significantly less trustworthy in handling personal information than in 2007 (35% versus 30% in 2013).

Chart 7. Trust in organisations to handle personal information



Base: All respondents

Q8 How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information?

Three additional types of organisation were included in this study, all of which were considered to be untrustworthy by the majority of Australians:

- Technology companies were more likely to be considered untrustworthy (49%) than trustworthy (37%).
- Debt collectors — only three in ten (31%) Australians considered debt collectors to be trustworthy.

- Social media organisations were considered to be trustworthy by only one in ten (9%) Australians.

There was a pattern of declining trust with increasing age in relation to nearly all types of organisations. The exceptions to this were retailers, where nearly a half of over 65 year olds said they were trustworthy (46%) and social media, where trust was highest amongst over 65 year olds.

Personal responsibility

Measures taken to protect personal information

Australians were asked how often, if ever, they took a number of measures in order to protect their personal information. Their answers are summarised in Chart 8, which shows the proportion of Australians who:

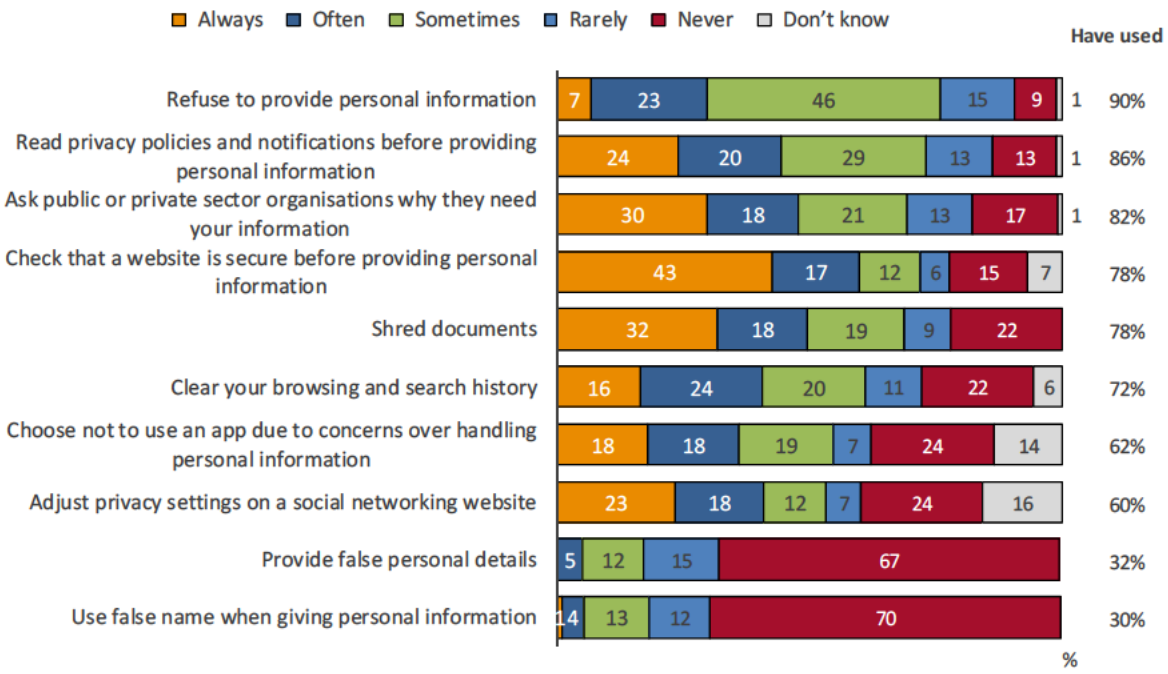
- refuse to provide personal information
- read privacy policies prior to providing personal information
- ask questions of organisations as to why particular information is needed
- shred documents
- check the security of a website
- clear their searching and browsing history
- choose not to use a smartphone app because of the information requested in order to use it
- adjust privacy settings on social networking sites
- provide false details
- provide a false name.

Only three people out of all the people interviewed claimed never to take any of these measures (less than 0.2%). However, while practically all Australians do something, they do not do everything routinely. Over four in ten (43%) said they "always" check that a website is secure before providing personal information, and around three in ten said they always shred documents (32%) or ask organisations why they need personal information prior to giving it (29%).

It is interesting to note that females (38%) are more likely to shred documents to protect personal information in comparison to males (25%). Four out of ten respondents (40%) aged 35+ years reported taking this measure in comparison to younger respondents aged 18-34 years (16%) and they were also more likely to read privacy policies with almost three out of ten people (29%) stating this in comparison to respondents aged 18-35 years (12%). On the other hand, younger respondents (aged 18-34 years) were more likely to check the security of a website than those aged 35+ years (51% and 38% respectively).

Fewer people provide false personal details (32%) and/or a false name (30%) to protect their privacy and less than one in twenty does so always or often. Similar questions were asked in 2007. Respondents were asked whether they have provided false personal details when completing online forms or applications as a means of protecting their privacy. Most respondents said 'no' (67%) while one in four (25%) said they have. However, just over six in ten people (61%) reported they intentionally leave some questions that ask for their personal details blank to protect their privacy.

Chart 8. Measures taken by Australians to protect their personal information



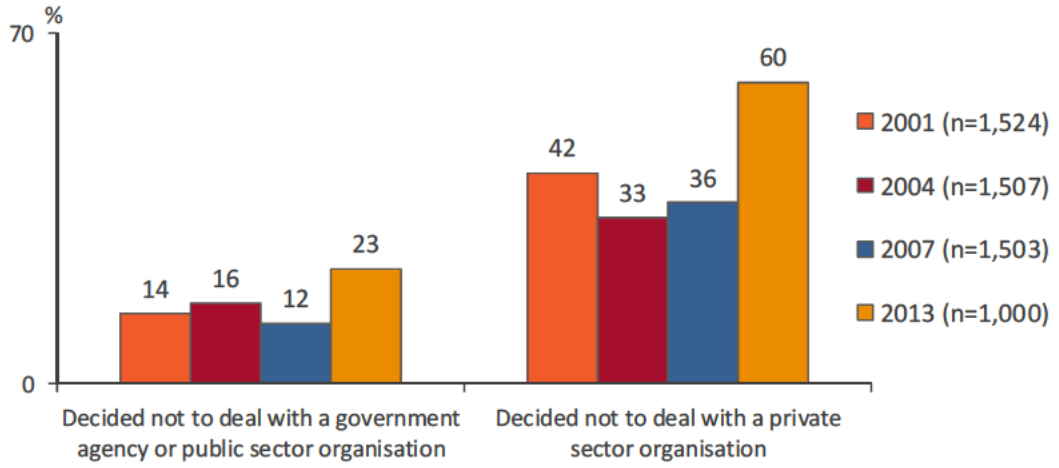
Base: All respondents (n=1,000)

Q21 In order to protect your personal information, do you...

Avoided dealing with organisations due to privacy concerns

Since 2001, Australians have been asked whether they have decided not to deal with either a government or private sector company because of concerns over the way that organisation might handle their personal information. Their responses are shown in Chart 9.

Chart 9. Australians who have decided not to deal with an organisation because of concerns over the use of personal information



Base: All respondents

Q18/19 Have you ever decided not to deal with a government agency or public sector / private sector organization because of concerns over the protection or use of your personal information?

These results indicate a significant change since 2007. While there have been increases amongst Australians of all types, there has been a significant rise in the proportion of people working in

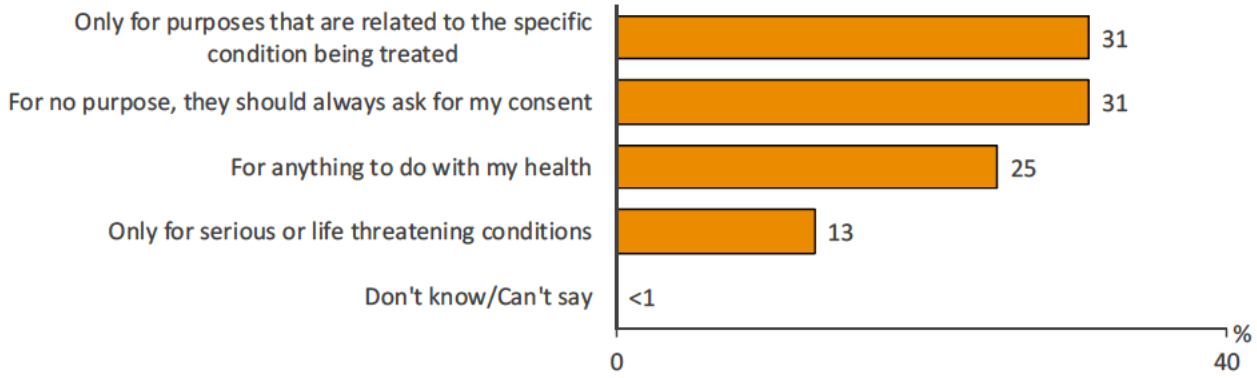
white collar occupations who have decided not to provide information to government or private sector organisations because of concerns over the use of that information from four in ten in 2007 (36%) to six in ten (60%). In total, just over six in ten (63%) Australians have decided not to deal with either type of organisation, up from four in ten (40%) in 2007.

Medical and health information

Health professionals sharing patient information

Respondents were asked to nominate which of four options best described their views on access to health information (multiple responses had been allowed previously).

Chart 10. Situations when transfer of health information is appropriate



Base: All respondents (n=1000)

Q22 Which of the following four options best describes when you think it would be ok for your doctor to share your health information with other health professionals?

Australians displayed quite different opinions with one in three saying that: such information could be transferred without their consent to treat the specific problem at hand (31%); or that consent should always be sought (31%). A quarter of people (25%) take a more relaxed approach, saying that they are happy for information to be shared between health providers for anything to do with their health. A further one in eight (13%) are happy for information to be transferred in serious or life-threatening cases. While the question was asked differently in previous surveys, the pattern of response is similar to the past.

In 2007, just over one in three people (35%) felt that the transfer of health information is appropriate when the purpose is related to the condition being treated. A similar proportion (25%) stated health information should not be transferred unless they ask the patient for their consent. One in four people were happy for their information to be transferred if it had to do with their health, while less than two in ten respondents (17%) said it would be acceptable if they had a serious or life threatening condition. There was no variation in gender or age.

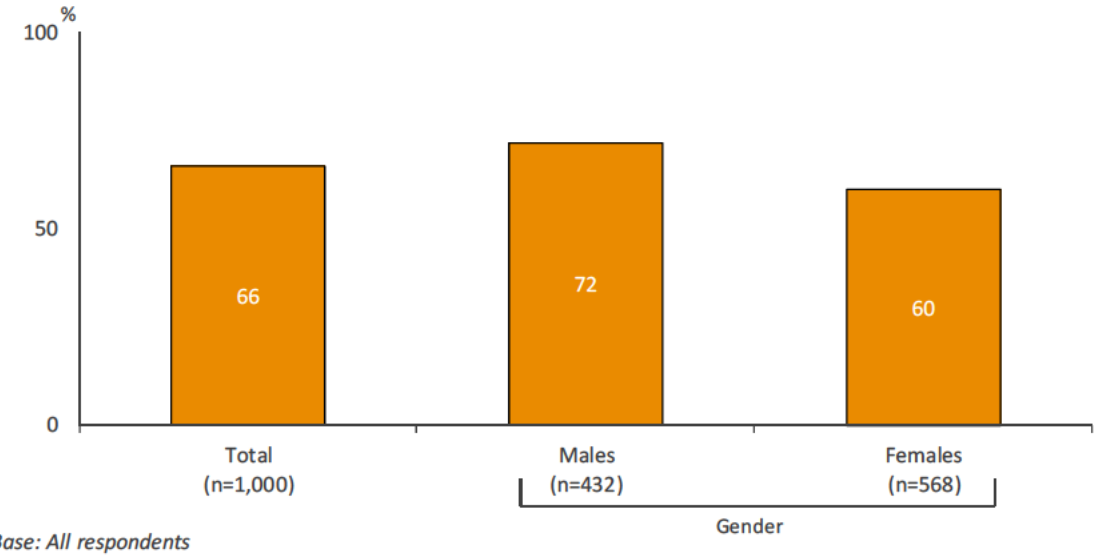
Health professionals discussing patient information

Chart 11 shows that the number of Australians prepared to accept their doctor discussing personal health details with other professionals without consent has increased over time from six in ten (59%) in 2007, to two thirds (66%) in 2013.

This shift has been driven by a large difference in the views of people at both ends of the working spectrum. Whereas in 2007, half (53%) of white collar and six in ten (59%) of blue collar workers agreed with this proposition, in 2013 the proportions are six in ten (63%) and three quarters (76%). People living in blue collar households remain the most accepting of this, but all other sectors of society have drawn closer in their opinions.

Women and men continue to hold slightly different views with seven in ten men (72%) and six in ten women (60%) now supporting their doctors discussing their health details without consent. This support has increased amongst both sexes since 2007 (64% and 55% respectively then).

Chart 11. Acceptability of doctor discussing personal medical details with other health professionals



Base: All respondents

Q23 To what extent do you think your doctor should be able to discuss your personal medical details with other health professionals in a way that identifies you without your consent if they believe this will assist your treatment?

Age does not seem to have a strong impact on this relationship. However, older people (aged 35+ years) were more likely to be accepting of their doctor discussing personal health details with other professionals without their consent (68%) in comparison to younger people (aged 18-34 years) (60%).

Privacy in the workplace

As technology develops new privacy issues have arisen, with employers able to access more information about their employees. This section examines some of these issues.

Random drug and alcohol tests

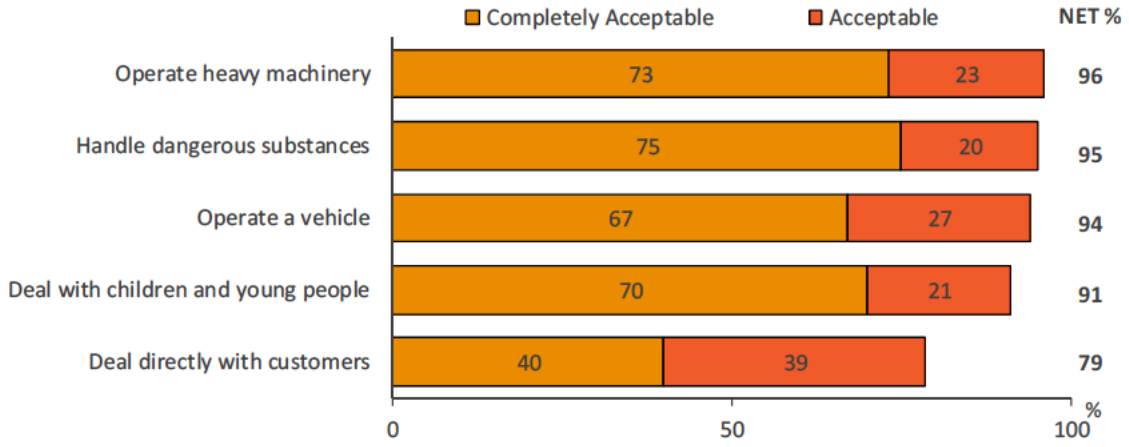
Most Australians, over nine in ten, believe it is acceptable for employers to carry out random drug and alcohol tests for employees who operate heavy machinery (96%), deal directly with children and young people (91%), operate a vehicle (94%) or handle dangerous substances (95%). With the exception of operating a vehicle, more than seven in ten people strongly agree with employers carrying out random drug and alcohol tests in these circumstances.

The proportion of people who stated it was 'completely acceptable' for employers to carry out random drug and alcohol tests for employees who operate a vehicle is close to seven in ten people (67%).

On the subject of dealing with customers, eight in ten (79%) agree that random drug and alcohol testing is acceptable, however, they are evenly divided between believing this is completely acceptable (40%) or just acceptable (39%).

The largest proportion of respondents who reported it is unacceptable for employers to carry out random drug and alcohol tests was for employees who deal directly with customers (19%). This was followed by nine out of ten people (9%) reporting random drug and alcohol tests is not acceptable for employees who deal directly with children and young people (9%), five out of ten people saying random tests are unacceptable for employees operating a vehicle (5%), employees handling a dangerous substance (4%) and those who operate heavy machinery (3%).

Chart 12. Acceptability of random drug and alcohol testing in the workplace



Base: All respondents (n=1000)

Q35 Thinking about random drug and alcohol tests in the workplace, do you think it is acceptable or unacceptable for employers to carry out these tests for employees who...

Workplace surveillance privacy policies

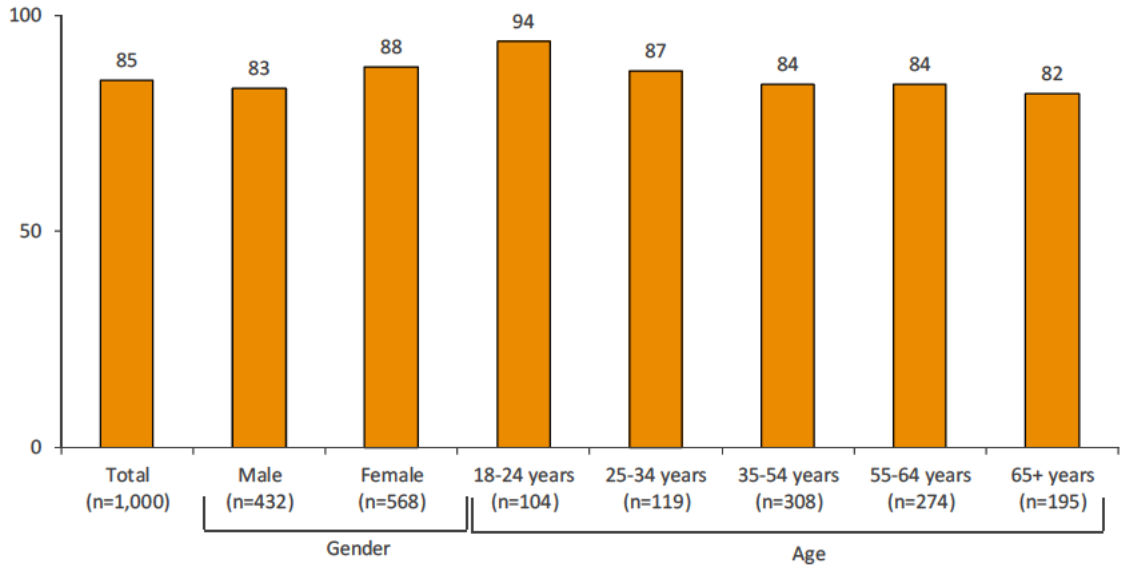
In 2007, people were asked for the first time whether they felt it is important for employers to have a privacy policy that covers when they will read emails, randomly drug test employees, use surveillance equipment to monitor employees, monitor telephone conversations and monitor activities in work vehicles via GPS.

The same question was asked again in this study and the results were very similar — nearly nine in ten Australians agree that employers should have such a policy (85%). The results were similar across the population in both the 2007 and 2013 survey, with a few exceptions:

- In 2007, 18–24 year olds placed the lowest level of importance on such policies (84%). This has changed and they now place the highest level of importance (94%), with the level declining with increasing age.

- In 2007, people living in households with incomes over $100,000 were the most likely to say these policies were very important (70%), whereas they now hold similar views to the rest of the population (although still significantly higher than low income households) (61%).

Chart 13. Consider it important that employers should have a policy covering surveillance practices



Base: All respondents

Q34 Thinking about the workplace, how important is it to you that an employer has a privacy policy that covers when they will read employee details, randomly drug test employees, use surveillance equipment to monitor employees and monitor telephone conversations and monitor GPS in work vehicles?

Identification document scanning

Acceptability of identification document scanning

In 2007, respondents were asked whether they felt it was acceptable to be asked to show or have a copy of identification documents made in a range of day-to-day circumstances. In 2013, the question was modified slightly to ask only about the acceptability of making a copy or scan of these documents.

The pattern of results between the two studies was similar. The greatest support for copying material was in order to obtain a credit card, which was considered to be acceptable by two thirds of the population (69% now compared with 57% in 2007). Support was lowest for purchasing general goods with only one in twenty (5% now and 4% in 2007) saying this is acceptable.

In general, Australians are more accepting of having their identification documentation copied compared to in 2007:

- An increase from 57% to 69% who say it is acceptable to scan or copy documentation in order to obtain a credit card.
- An increase from 23% to 31% for people who believe it is acceptable when purchasing goods that require the purchaser to be over 18.

- An increase from 18% to 28% in those finding it acceptable to have their identity documents copied in order to enter licensed premises (e.g. pub, club or hotel).

Table 10. Attitudes towards scanning or copying identification documents

Q36 items	Acceptable %	Not Acceptable %	Don't Know %
To purchase general goods	5	95	1
To purchase cigarettes	24	75	1
On entry to licensed premises	28	72	1
To purchase good for which you need to be over 18	31	67	2
To obtain a credit card	69	29	2

Base: All respondents (n=1000)
Note: Multiple responses given
Q36 In which of the following situations, if any, do you think it is acceptable that a COPY or SCAN is made of your identification documents?

There are a few differences of opinion within the community on this issue. In particular, people who are working are significantly more likely to support having identification documents scanned in order to obtain a credit card (72%) compared with those who are not working (64%).

The opposite position is true for purchasing goods for which you need to be aged 18 or over, where people who are working find this significantly less acceptable (29%) than those who are not working (36%). The acceptability of having identification documentation copied in order to be able to buy general goods (e.g. clothing and food) declines from nearly one in ten (9%) people educated up to Year 10 to one per cent of people who have completed postgraduate studies.

Biometrics

The use of biometric data is increasing at a rapid rate. For example, it is now common practice to be required to provide such information in order to travel internationally. Australians were asked to indicate how concerned they are about having to provide biometric data, including their fingerprints, photo ID or iris scans in a number of different situations.

Australians were not keen on the need to use this data to gain access to a pub, club bar or hotel, with seven in ten (71%) being either very concerned (41%) or somewhat concerned (28%) at this prospect. The level of concern was consistent across age groups, but there were higher levels in New South Wales (76%), and South Australia and the Northern Territory (77%).

Over half of the population was concerned about having to use biometric information to access their place of work or study (55%) or to do their day to day banking (54%). 18–24 year olds were the most concerned with both ideas, with concern declining with age. However, concern was at over 50% for all age groups.

The majority of respondents were less concerned by the use of biometric information to get on a flight, with four in ten people saying they were concerned — women (44%), significantly more than men (36%).

One in five people had no concerns about the use of biometric information in any of the situations suggested to them (20%). This was true across all demographic categories, although those with no concerns were more likely to be Queenslanders (27%).

Table 11. Concern with using biometric data in a number of day to day situations

Q37 items	Very Concerned %	Somewhat Concerned %	Not Concerned %	Don't Know %
Go into a licenced bar, club or hotel	43	28	29	1
Get into your place of work or study	25	30	43	2
Do your day to day banking	25	28	45	2
Get on a flight	17	23	59	<1

Base: All respondents (n=1000)

Q37 How concerned are you about using biometric information for you to…

Internet and smartphones

The way in which people access the internet has changed dramatically since the last survey. A number of factors have contributed to this, including a significant growth in the use of social networking sites and the development of smartphone and tablet technology.

According to a recent report by the Australian Communications and Media Authority (ACMA), by May 2012 almost half of adult Australians had a smartphone and they were being used increasingly to access the internet (ACMA, *Communications Report 2011-12 Series. Report 3 – Smartphones and Tablets*, 2012). Whereas mobile phones were used largely to make calls or send SMS messages or emails, the raft of services now available on smartphones and other mobile platforms is enormous, as is the amount of personal information that is being transmitted through them.

The series of questions posed in the 2007 study has been augmented and changed to reflect the different circumstances now.

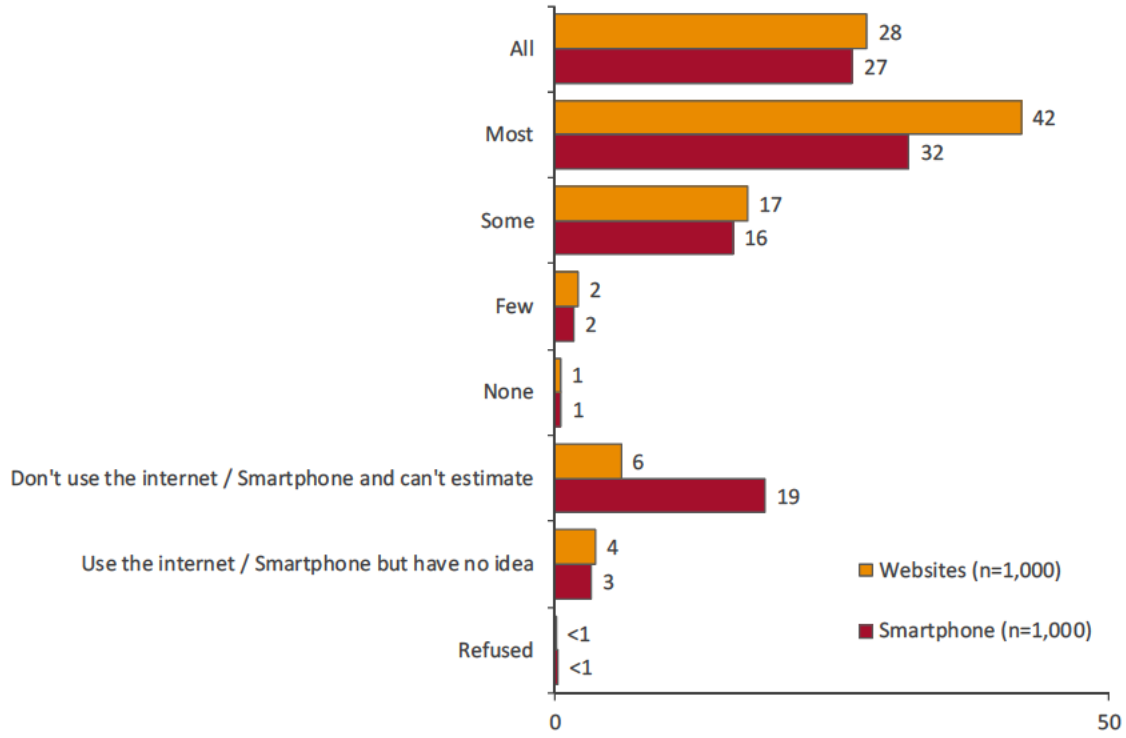
Understanding of passive data collection on the internet

For the first time, Australians were asked to estimate the proportion of websites and smartphone applications (or apps) that collect information about users.

As Chart 14 shows, over a quarter of the population believes that **all** websites and Smartphones collect personal information about them. In addition, almost a further six in ten believe that most (42%) or some (17%) websites collect information and nearly half (48%) believe that most (32%) or some (16%) smartphones apps collect information about users of them.

Survey participants were encouraged to make an estimate even if they were not users of the technology themselves. However, those who simply could not make an estimate were asked whether they used the technology or not and the majority said that they could not estimate because they did not use these technologies.

Chart 14. Proportion of websites or Smartphones that collect information about users



Base: All respondents

Q24/24a What proportion of websites/smartphone apps do you think collect information about the people who visit/use them?

Online tracking and behavioural advertising

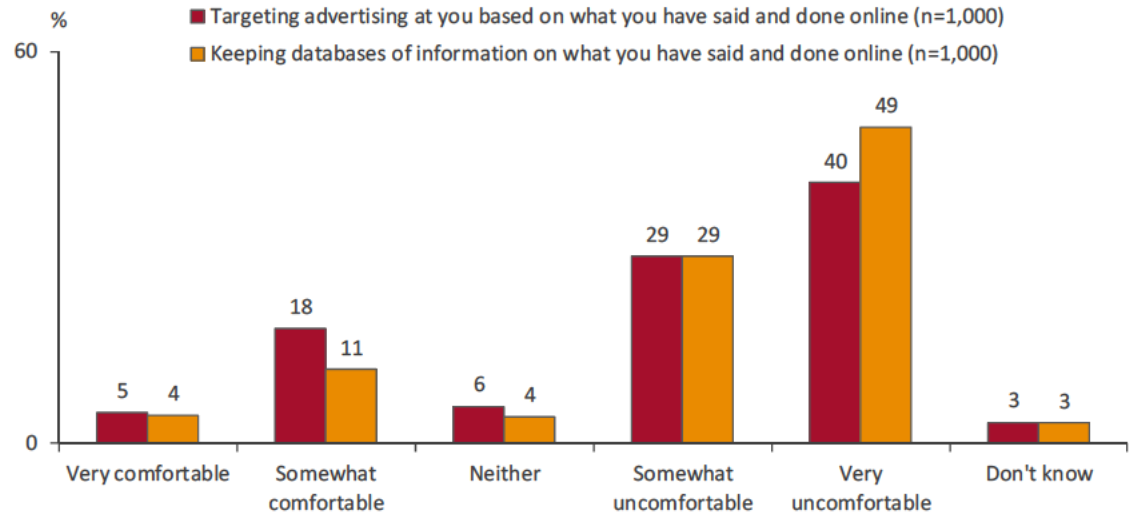
Participants were introduced to the concept that search engines and social networking sites track patterns of usage on the internet and maintain databases of information about users to enable sites to target advertising and other offerings to website users. They were then asked to comment.

Chart 15 shows that Australians are generally uncomfortable with the prospect of information being captured and used to target advertising and other offerings to them. They are marginally more comfortable with the concept of having advertising targeted to them based on their online activities, rather than the prospect of having their online activities stored in a database for non-specific purposes — nearly half of the population felt very uncomfortable at this prospect (49%).

Nonetheless, a quarter of the public is comfortable with targeted advertising based on internet behaviour at the time of using the internet (25%), although three in ten people under the age of 55 (27%) are comfortable compared with less than one in seven aged 55 or over (15%).

A slightly smaller proportion is comfortable with browsing behaviour being stored for later targeting (15%). Again people aged under 55 (19%) are more comfortable with this idea and they are twice as likely to be comfortable with this than people aged over 55 (9%).

Chart 15. Degree of comfort with tracking and storing online behavior



Base: All respondents

Q25 How comfortable are you with.....?

Providing personal information online

In 2007, participants were asked whether they were more or less concerned about providing information electronically or online compared to in hardcopy or paper. The situation remains unchanged with two thirds of Australians (67%) saying they are more concerned about providing information electronically or online, than via hardcopy.

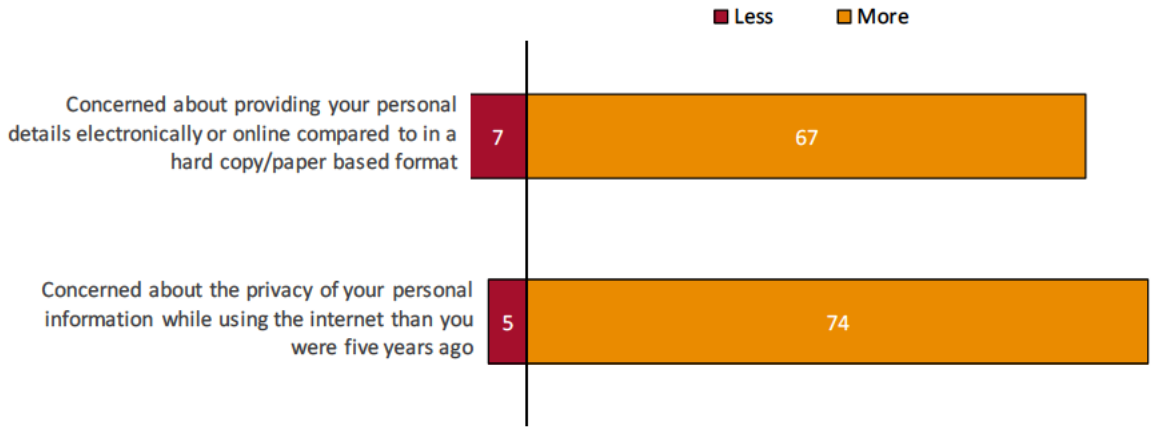
People living in households earning under $75,000 remain the most sceptical about the electronic or online provision of personal information, with over seven in ten (72%) people saying they are more concerned when using this format than paper.

In 2007, survey participants were asked whether they were more or less concerned about providing information via the internet than they were two years earlier. A half of Australians (50%) said that they were more concerned — nearly five times as many as the proportion whose concerns had lessened (11%).

Given the interval between surveys, and the substantial changes to technologies in the last few years, participants were asked the same question in 2013 but instead of two years, were asked to consider their position now relative to five years ago. Chart 16 shows that three quarters of people (74%) are more concerned than they were five years ago. This change may reflect the increased timeframe or the data environment. Levels of concern are similar across the board. Only one in twenty participants (5%) claims to be less concerned now than they were five years ago.

The responses of those who felt there had been no change are not shown in Chart 16. On average, a quarter of the population, saw paper and online data collection as being the same (24%), however people living in households earning more than $75,000 were more likely (28%) not to have noted a difference.

Chart 16. Change in level of concern for providing information over the internet in different forms



Base: All respondents (n=1000)

Q28/29 Are you more or less concerned about providing your personal details electronically or online compare to in hard copy format/ compared with five years ago

One in six Australians (18%) said that they there were no more or less concerned about the privacy of their personal information than they were five years ago. Men were especially likely to have noted no change (21%).

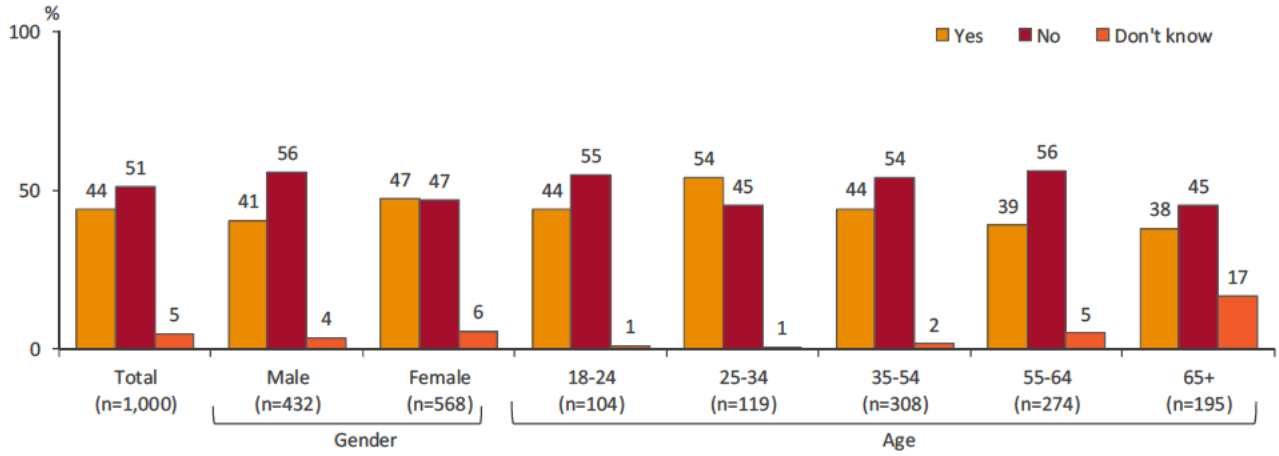
Privacy policies on websites

While the majority of Australians continues to *not* read privacy policies, the proportion has declined from nearly six in ten (59%) in 2007 to around half (51%) in 2013. Overall, just over four in ten (44%) Australians claim to read website privacy policies. Australians' tendency to read them varied along demographic and attitudinal lines.

- Readership of privacy policies relates to internet usage, with Australians aged over 65 being the least likely to read them (38%).
- Females (47%) are more likely to read them than males (41%).
- Australians with a bachelor degree (46%) or postgraduate qualification (51%) were more likely to read privacy policies than those who had been educated up to year 10 (34%).
- Experience and behaviour also played a role in propensity to read privacy policies, with those who had boycotted a private company (51%), public organisation (61%), had experienced a problem with personal information (52%) or had some experience of identity theft (51%) being most likely to read privacy policies.

The survey participants who read website policies were asked to describe the impact these have on them. The main response was that they help respondents to make a decision on whether or not to use the site (at 37% an increase from 27% in 2007). Some respondents reported that reading privacy policies gives them more confidence about using the site (15%) — this has decreased from 2007 (25%).

Chart 17. Profile of privacy policy readers



Q30 Do you normally read the privacy policy attached to any internet site?

Table 12. Impact of seeing or reading privacy policies on attitudes towards the site.

Q31. What impact, if any, did seeing or reading these privacy policies have upon your attitude towards the site?	Total (n=429) %
Helps me decide whether to use the site or not	37
Feel more confident/comfortable/ secure/ about using site	15
No real impact/ no change	13
Made me more cautious/ aware when using the internet generally	11
It's a good idea/ I approve of the privacy policy they are doing the right thing/ prefer to see on sites/ respect site for having it	8
Still apprehensive about sites that have them/ don't trust them/ not convinced	7
Appear more honest/ trustworthy/ responsible/ legitimate	5
Too long/ complicated to read	5
Unable to enter site without reading it	1
It depends/ varies	1
Doesn't mean much/ legal obligation	1
Other	4
Don't know	8

Base: Respondents who normally read privacy policies
Note: Multiple responses given

Amongst the majority who choose not to read privacy policies, the main reason for this by far is that **they are too long** (52%) and, related to this, that they are **complicated** (20%) and **boring** (9%). One in ten respondents said that they don't use the internet — this is the same proportion of respondents who claimed not to use the internet throughout this study.

Other reasons were given by around one in twenty respondents or less, but they group into several key themes. The main reason is that some readers are discerning and read some policies but not

others depending on the nature of usage of the site or knowledge of the site. There is also an element of mistrust — some people said that there is little point in reading a privacy policy that the organisation will not comply with or has taken no care in writing. Having difficulty finding policies on websites is also a deterrent for some people as well as having difficulty reading them.

Table 13. Reasons for not reading privacy policies

Q32. Why don't you read website policies?	Total (n=515) %
Too long	52
Too complex	20
Don't use internet or computer	11
Too lazy/ can't be bothered/ boring	9
No need if I trust the organisation	6
Hard to find	5
Agencies and organisations don't comply with them	5
I don't use sites that have or need them	5
Difficult to read small font	3
They are all the same	3
I don't give out information online	2
Do read on some websites	2
I have never seen one	1
No reason	1
Other	4
Don't know	<1

Base: Respondents who don't normally read privacy policies
Note: Multiple responses given

Social networking

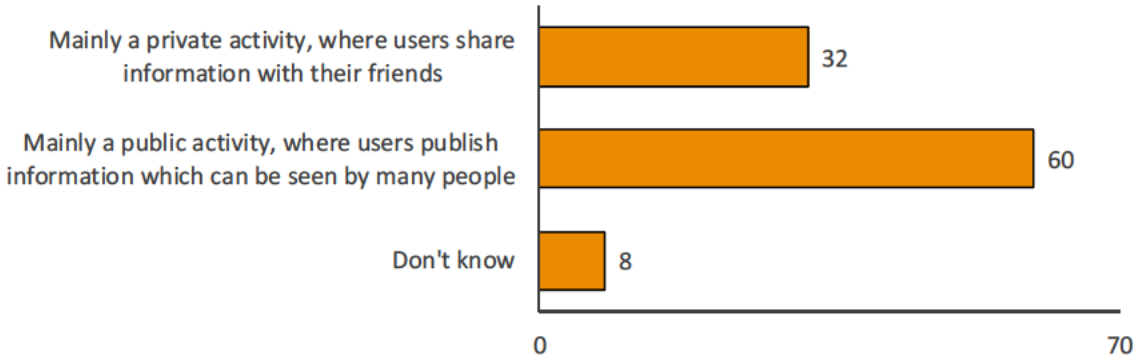
In 2007, social networking site Facebook had 21 million registered members[5]. This number has risen to over 980 million now. LinkedIn reports more than 200 million acquired users in more than 200 countries and territories, up from 17 million in early 2007[6].

Community understanding of how social networking sites operate is essential to helping people use social networks in a manner that protects their personal information.

Not surprisingly, when asked whether they had ever posted anything on a social networking site that they later regretted there was a direct relationship with age — the older a person the less likely they are to have regretted something they have posted online.

[5] Lange, Ryan. and Lampe, Cliff. *"Feeding the Privacy Debate: An Examination of Facebook"* Paper presented at the annual meeting of the International Communication Association, TBA, Montreal, Quebec, Canada, May 22, 2008: p.20
[6] http://www.examiner.com/article/linkedin-steps-up-security-with-new-safety-protocols

Chart 18. Understanding of what social networking is

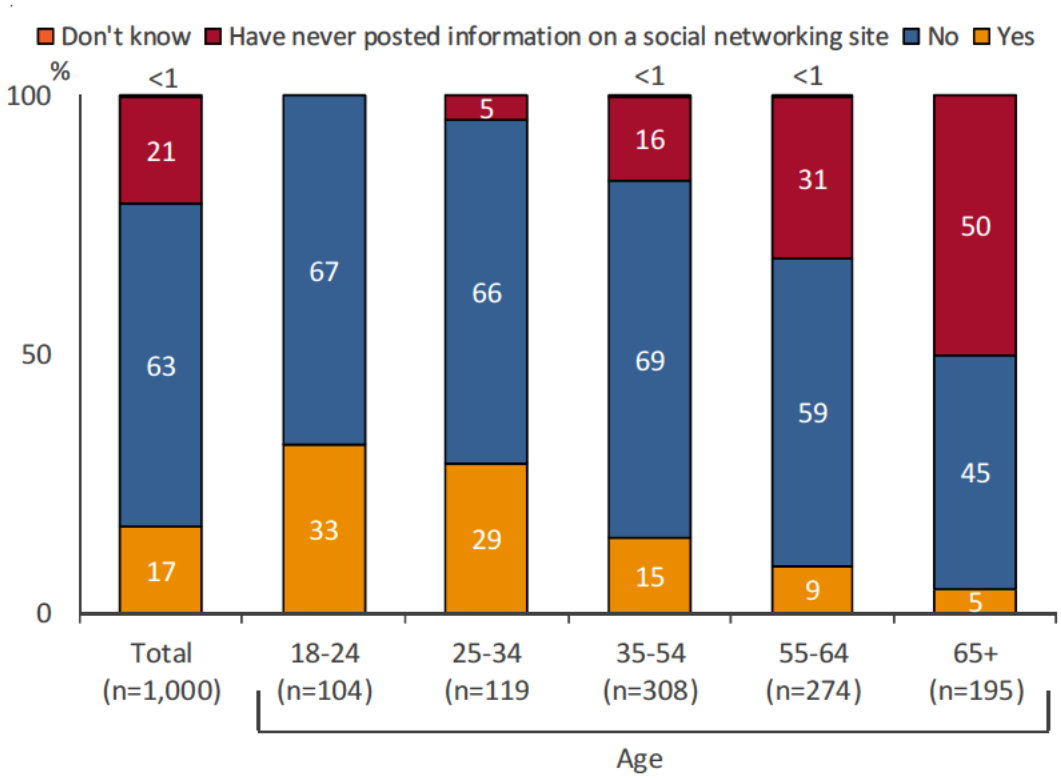


Q27 Do you think that social networking is...?

Chart 18 shows that the majority of people (60%) believe that social networking sites are mainly **public** activities. These views were held consistently across the community.

The slightly less than one in ten people overall who were unable to answer this question were predominantly aged over 55.

Chart 19. Proportion regretting social networking posts



Base: All respondents (n=1000)

Q26 Have you ever put any information on a social networking site that you've later regretted sharing with others?

On average, slightly under one in twenty Australians (17%) confirmed that they had regrets about something they had posted, but this figure increased to a third of young adults aged under 24 (33%). A half of people aged over 65 had **never** posted anything to a social networking site.

ID theft and fraud

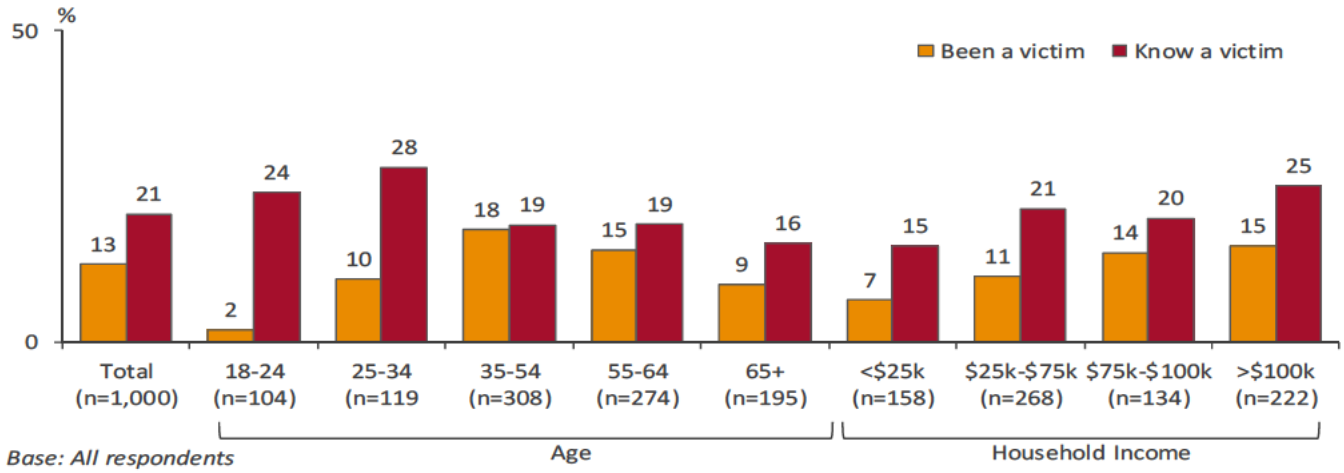
Since the last study was undertaken in 2007, the Australian Bureau of Statistics (ABS) has introduced a regular survey to estimate the incidence of ID fraud and theft in Australia (CAT No. 4528.0). The first ABS measure was taken in 2007 at a similar time to this study. At that time, one in twenty Australians aged 15 or over (5%) recorded having been the victim of ID fraud and theft, credit card theft or scams in the previous year. In its latest release, based on data collected in 2011, this figure had risen (7%). ID theft is growing at the slowest rate (0.8% in four years), but fraud related to identity, credit cards and scams is growing more quickly (2–3 % over a four year period).

When this study asked adult Australians if they had **ever** been the victim of ID fraud or theft or whether they know someone who has, one in eight (13%) said that they had been a victim themselves (up from 9% in 2007) and one in five (21%) said it had happened to someone they know (up from 17% in 2007). The trends are thus the same and now a third (33%) of the population has either been the victim of ID fraud or theft or knows someone who has.

The characteristics of victims are consistent with the ABS, and for this study are:

- Men (14%) and women (11%) are equally likely to be the victim.
- Victimisation rates are lower for people aged under 25 (2%) and over 65 (9%).
- Victimisation rates increased with household income (7% of those living in households earning less than $25,000 versus 15% of those living in households earning more than $100,000).

Chart 20. Proportion of Australians who have been or know someone who has been the victim of ID fraud and theft



Base: All respondents

Q38 Have you (or someone you personally know) ever been the victim of identity fraud or theft?

Australians are generally becoming more concerned about identity theft or fraud. In total, over two thirds of Australians expressed concern about the possibility of becoming the victim of ID theft and fraud in the next year (69%) a significant change compared with 2007 (60%).

Another significant change is the level of concern — a quarter of people interviewed in 2013 said they were "very concerned" (25%) compared with one in six (17%) in 2007. As was the case in 2007, the people who are least likely to be the victims of ID fraud and theft are those most concerned about the possibility of it happening to them.

A quarter of people aged under 35 know a victim (25%), but a much lower percentage has been the victim themselves. Nonetheless, younger Australians are the least likely to think that they may become the victim of ID theft and fraud in the next 12 months.

Australians living in Western Australian were most likely to have been a victim of identity theft (18%) or know someone who was (40%). This is similar to 2007 where one in seven (14%) WA residents had been a victim.

Credit reporting

The Privacy Act provides safeguards for individuals in relation to consumer credit reporting. In particular, Part IIIA governs the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies (CRAs), credit providers and a limited number of other recipients.

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* contains significant changes to the current credit reporting regime. While the bulk of the changes have not yet come into effect, the credit reforms came into effect from the passing of the Act. This means that from December 2012, information relating to individuals' repayment histories will become part of the new more comprehensive reporting structure.

Given that the provisions are yet to come into effect, it was considered timely to ask Australians to comment on their understanding of the law, so that changes in attitudes and understanding may be measured in future.

As this was the first time these questions have been asked in this study, and to ensure that respondents understood the line of questioning, they were told:

> *I'd like to ask you a few questions now about credit ratings and information that organisations use to work these out. Most people who have rented a house, paid bills for utilities or borrowed money have a credit rating. The information needed to build this rating is available in a credit report.*

People were read three statements about how credit reports might work. A quarter of Australians (26%) selected that *everyone is able to see credit information held about them and they are able to get this from the organisation free of charge*. This view was widely held amongst Australians of all types, although a higher proportion of people called on their mobile phone agreed with this option (34%) as well as males (29%).

The majority opted for the statement *everyone is able to see credit information held about them but they may have to pay a fee to the organisation that holds the information.* Nearly half of the community chose this (48%) and working Australians, especially those living in high income households were the most likely to choose it (57% of those living in households earning more than $75,000).

The option that *no-one can get access to credit information whether they're prepared to pay for it or not* was chosen by one in six Australians (17%), rising at both ends of the age spectrum to over one in five younger Australians (22% of 18–24-year-olds) and a quarter of older Australians (aged 65+) (26%).

One in ten Australians were unable to respond (9%). Women (13%) and older Australians (17% of over 65 year olds) were the least likely to choose one of the three options.

The oldest (92% of those aged over 65 years) and youngest adult Australians (96% of those aged between 18 and 24 years) were the least likely to have tried to get access to their credit reports. Overall, one in six Australians had tried to access their credit report (17%) and subsequent questioning asked these people to describe their experiences. The group most likely to have accessed their report were aged 25–55 with around a quarter of people in this age range having accessed one.

Not surprisingly, given this age range, working Australians (20%) were more likely to have gained access than non-working Australians (13%). Otherwise people came from all walks of life. One characteristic of this group is that they were much more likely than those who had not accessed their credit report to have:

- refused to give information to public companies because of concerns over the use of their information (30% versus 23% overall)
- had problems with personal information handling (49% versus 33% overall)
- read an online privacy policy (55% versus 44% overall)
- been the victim of ID fraud or theft (21% versus 13% overall).

The one in six (17%) Australians who had accessed their credit report experienced the following:

- Just over four in ten (43%) were charged for access to their data (7% of the population)
- Seven in ten (70%) found the information on the report to be correct
- Of the three in ten (30%) who found it to be incorrect:
    - Nearly six in ten (57%) were able to have the information corrected
    - Just over half (55%) made a complaint about the fact that the information was incorrect. Of these, the majority made that complaint to the organisation involved (41%), with others complaining to a credit report organisation (25%), the financial institution (19%), the Ombudsman (12%) or a government department (3%).

Office of the Australian Information Commissioner

GPO Box 2999, Canberra ACT 2601
GPO Box 5218, Sydney NSW 2001

For further information
tel: 1300 363 992
email: enquiries@oaic.gov.au

or visit our website at
www.oaic.gov.au

5.0 Appendix 1: Questionnaire

THE AUSTRALIAN GOVERNMENT
OFFICE OF AUSTRALIAN INFORMATION COMMISSIONER

COMMUNITY ATTITUDES TO PRIVACY SURVEY 2013

FINAL
QUESTIONNAIRE
13 June 2013

COMMUNITY ATTITUDES TO PRIVACY SURVEY 2013

Good morning/afternoon/evening. My name's ……. from Wallis market and social research in Melbourne. We're doing a confidential study on privacy for the Office of the Australian Information Commissioner (if necessary — the privacy regulator) about the protection and use of people's personal information by government and businesses. It'll take about 25 minutes. Is now convenient?

TELL RESPONDENT SAMPLE DETAILS, DATA STORAGE DETAILS, AMSRS SURVEYLINK NUMBER, STRESS WALLIS IS AMSRO MEMBER AND STUDY IS IN KEEPING WITH NPPS AND WALLIS 1800 NUMBER AS REQUIRED

IF NOT AVAILABLE MAKE APPOINTMENT

S1 To make sure that we speak with a wide range of people from the community can I ask you which one of the following broad age groups you belong to (READ OUT)?

18 to 24.....1 CHECK QUOTAS
25 to 34.....2 CHECK QUOTAS
35 to 54.....3 CHECK QUOTAS
55 to 64.....4 CHECK QUOTAS
Over 65.....5 CHECK QUOTAS
Refused (DO NOT READ OUT).....6 TERMINATE
Under 18 (DO NOT READ OUT).....7 TERMINATE

S2 RECORD GENDER

S3 What is your postcode (Check location quotas)

MONITORING

This call will be recorded and may be monitored for quality control purposes. Please could you tell me if you do NOT want this to happen?

DO NOT MONITOR..... 1
OK to monitor 2

GENERAL ATTITUDES TOWARDS COLLECTION AND USE OF PERSONAL INFORMATION

In Australia, privacy law relates to the protection of an individual's 'personal information'. This is any information about you that identifies you or could reasonably be used to identify you. For example, this includes things like:

- your name or address
- financial details
- photos
- your opinions and beliefs
- membership of groups and affiliations
- racial or ethnic origin
- health information (including genetic information)
- sexual preferences
- criminal record.

Note: *#OPC before the question number indicates that the question was asked in 2007*

Q1 **I'd like to start by asking you what you think are the biggest privacy risks that**

MULTI

Online services/social media sites 1
Workplace privacy 2
ID scanning 3
ID theft/fraud 4
Data security/data breaches 5
Credit reporting 6
Smart phones/apps 7
Surveillance 8
Sending information overseas 9
Other (specify) 10
Don't know 99

#OPCQ2.	Now I'd like you to think about providing your personal information to any business, organisation or government agency, IN GENERAL, what types of information are you reluctant to provide? (DO NOT READ) (MULTI)

Name 1
Address.....2
Email address.....3
Phone number.....4
Financial details.....5
Marital status.....6
Date of birth.....7
Medical information.....8
Genetic information.....9
Religion.....10
How many people/men/women in the household.....11
Other (specify).....12
Don't know.....99

IF NONE/DK GO TO Q6, IF SINGLE RESPONSE GO TO Q4, IF MULTI RESPONSE CONTINUE

#OPCQ3.	And which ONE of these [list answers given for Q2] do you feel MOST RELUCTANT to provide?

Name 1
Address.....2
Email address.....3
Phone number.....4
Financial details.....5
Marital status.....6
Date of birth.....7
Medical information.....8
Genetic information.....9
Religion.....10
How many people/men/women in the household.....11
Other (specify).....12
Don't know.....11

#OPCQ4.	What is your MAIN reason for not wanting to provide [answer from Q3]? (DO NOT READ)

May lead to financial loss/people might access bank account 1
It's none of their business/privacy 2
Discrimination 3
I do not want to be identified 4
I do not want people knowing where I live or how to contact me 5
The information may be misused/information might be passed on without my knowledge 6
Don't want junk mail/unsolicited mail/SPAM 7
I don't want to be bothered/hassled/hounded by phone or door to door 8
For safety/security/ protection from crime 9
Unnecessary/irrelevant to their business or cause ... 10
Other (specify) 11
Don't know 99

Now I'd like you to think about laws that relate to your privacy and personal information.

#OPCQ6.	Were you aware that there are Federal PRIVACY LAWS before this interview?

Yes 1
No 2
Don't know 99

TRANSFER OF PERSONALISED INFORMATION

Many organisations handle personal information.

#OPCQ8. **Thinking now about trustworthiness. How trustworthy or untrustworthy would you say the following organisations are with regards to how they protect or use your personal information? (ROTATE)**

(IF TRUSTWORTHY: Is that very trustworthy or somewhat trustworthy?
IF UNTRUSTWORTHY: Is that very untrustworthy or somewhat untrustworthy?)

	Very Trust	S'what Trust	Neither	S'what UnT	Very UnT	Don't know
Financial institutions	1	2	3	4	5	99
Real Estate Agents	1	2	3	4	5	99
Insurance Companies	1	2	3	4	5	99
Charities	1	2	3	4	5	99
Government Departments	1	2	3	4	5	99
Health service providers including doctors, hospitals and pharmacists	1	2	3	4	5	99
Market and social research organisations	1	2	3	4	5	99
Retailers	1	2	3	4	5	99
eCommerce industry, (including businesses selling over the internet)	1	2	3	4	5	99
Social media industry	1	2	3	4	5	99
Organisations that are provided with personal information to collect debts	1	2	3	4	5	99
Technology companies (eg software companies and online services such as email)	1	2	3	4	5	99

***[Rotate Q9-11]**
#OPCQ9. **GENERALLY, how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive discounted purchases?**
(Is that very or somewhat?)

Very likely 1
Somewhat likely 2
Neither likely nor unlikely 3
Somewhat unlikely.....4
Very Unlikely 5
Don't know.....99

#OPCQ10.	How about if it meant you would have a chance to win a prize? (Is that very or somewhat)

Very likely **1**
Somewhat likely **2**
Neither likely nor unlikely **3**
Somewhat unlikely **4**
Very Unlikely **5**
Don't know **99**

Q11.	And how likely or unlikely would you be to provide your personal information to an organisation if it meant you would receive better service, for example, being able to use more functions on a website, or receive improved customer service? (Is that very or somewhat)

Very likely **1**
Somewhat likely **2**
Neither likely nor unlikely **3**
Somewhat unlikely **4**
Very Unlikely **5**
Don't know **99**

#OPCQ12. Thinking now about the way that your personal information is handled by private or public sector organisations, which of the following instances would you regard to be a misuse of your personal information? (ROTATE)

	Yes	No	Don't know
An organisation that you haven't dealt with gets hold of your personal information	1	2	99
An organisation monitors your activities on the Internet, recording information on the sites you visit without your knowledge	1	2	99
You supply your information to an organisation for a specific purpose and they use it for another purpose.	1	2	99
An organisation asks you for personal information that doesn't seem relevant to the purpose of the transaction.	1	2	99
An organisation reveals a customer's information to other customers	1	2	99
An organisation sends customer data to an overseas processing centre	1	2	99

#OPCQ13.	How concerned are you about Australian organisations sending their customers' personal information overseas? Is that very or somewhat?

Very concerned 1
Somewhat concerned 2
Not concerned 3
Don't know 99

Q14.	I'd like you to think about the way that your personal information is handled by private sector organisations and government agencies. Please tell me if you agree or disagree with the following statements. (ROTATE) (Is that strongly or somewhat..?)

	Strongly agree	Some what agree	Neither	Some what disagree	Strongly disagree	Don't know
It's extremely important that private sector organisations tell me how they protect and handle my personal information	1	2	3	4	5	99
If a government agency loses my personal information they should tell me	1	2	2	2	5	99
If a business loses my personal information they should tell me	1	2	3	4	5	99
It's extremely important that government agencies tell me how they protect and handle my personal information	1	2	3	4	5	99

#OPCQ33.	Thinking about direct marketing. Which of the following statements BEST DESCRIBES how you GENERALLY feel when organisations that you have NEVER DEALT WITH BEFORE send you unsolicited marketing information? Would you say you feel … (READ OUT)

Annoyed.....1

Concerned about where they obtained it.....2

It doesn't bother you.....3

It's a bit annoying but it's harmless.....4

You don't mind getting it at all.....5

Or something else (specify).....6

Don't know (DO NOT READ).....99

I'd like you to think now of steps you've taken to protect your personal information.

Q21. **I'm going to read you a list of things you might have done. In order to protect your personal information how often, if ever, do you.. (READ OUT)? (ROTATE) Would that be always, often, sometimes, rarely or never?**

	Always	Often	Some times	Rarely	Never	Don't know
Shred documents	1	2	3	4	5	99
Check that a website is secure before providing personal information (eg check for security encryption)	1	2	3	4	5	99
Ask public or private sector organisations why they need your information	1	2	3	4	5	99
Read privacy policies and notifications before providing personal information	1	2	3	4	5	99
Use false name when giving personal information	1	2	3	4	5	99
Provide false personal details	1	2	3	4	5	99
Refuse to provide personal information	1	2	3	4	5	99
Adjust privacy settings on a social networking website	1	2	3	4	5	99
Clear your browsing and search history	1	2	3	4	5	99
Choose not to use an app (application) on a mobile device because of concerns over handling your personal information	1	2	3	4	5	99

*[rotate Q18 and Q19]

#OPCQ18.	Have you ever decided NOT TO DEAL with a government agency or public sector organisation because of concerns over the protection or use of your personal information?

Yes.....1
No.....2
Don't know.....99

#OPCQ19.	And have you ever decided NOT TO DEAL with a private sector organisation because of concerns over the protection or use of your personal information?

Yes.....1
No.....2
Don't know.....99

DEALING WITH COMPLAINTS AND PROBLEMS

Now I'd like you to think about your own experiences with personal information.

Q15.	Have you experienced a problem with how your personal information was handled in the past 12 months?

Yes.....1
No.....2
Don't know.....99

#OPCQ17.	If you wanted to report misuse of your personal information to someone, who would you be MOST likely to contact?

MULTI

Police 1
Ombudsman 2
The organisation that was involved 3
The Privacy Commissioner (Federal or State) 4
Consumer Affairs (in your state) 5
Federal/Local/State MP 6
Other Government department 7
Local Council 8
Lawyers/solicitors 9
Department of Fair Trading 10
The media e.g. TV/ radio/ newspapers 11
Seek advice from a friend or relative 12
Other (specify 13
Don't know 99

Information about your health is considered sensitive under the Privacy Act.

#OPCQ22.	Which of the following four options best describes when you think it would be OK for your doctor to share your health information with other health professionals (including pharmacists, specialists, pathologists or nurses), …..(READ OUT)? (SINGLE RESPONSE)

For anything to do with my health care 1
Only for purposes that are related to the specific condition being treated 2
Only for serious or life threatening conditions 3
For no purpose, they should always ask for my consent 4
Don't know 99

#OPCQ23.	To what extent do you agree or disagree that your doctor should be able to discuss your personal medical details with other health professionals - in a way that identifies you - WITHOUT YOUR CONSENT if they believe this would assist your treatment? Is that strongly or somewhat?

Strongly agree.....1
Somewhat agree 2
Neither agree nor disagree 3
Somewhat disagree 4
Strongly disagree.....5
Don't know.....99

#OPCQ34.	Now thinking about the workplace, how important is it to you that an employer has a privacy policy that covers when they will read employee emails, randomly drug test employees, use surveillance equipment to monitor employees, monitor telephone conversations and monitor GPS in work vehicles. Is it….

Very important.....1
Quite important 2
Not very important 3
Not at all important 4
Don't know (DO NOT READ) 99

Q35.	Now thinking about random drug and alcohol tests in the workplace, Do you think it is acceptable or unacceptable for employers to carry out these tests for employees who… (READ OUT) (RANDOM) Is that completely acceptable, acceptable or unacceptable

Operate heavy machinery 1
Operate a vehicle 2
Deal directly with customers 3
Deal directly with children and young people.....4
Handle dangerous substances.....5

INTERNET AND SMARTPHONES

Q24.	Thinking now about using the internet. What proportion of websites do you think collect information about the people who visit them? Would you say it is (READ OUT)

All 1
Most 2
Some 3
Few 4
None 5
Don't use the internet and can't estimate 6
Use the internet but have no idea 7
Refused 99

Q24a.	Now thinking about your Smartphone. What proportion of smart phone apps collect information about the people who use them? Do you think it is…(READ OUT)

All 1
Most 2
Some 3
Few 4
None 5
Don't have a smartphone and can't estimate 6
Have a smartphone but have no idea 7
Refused 99

Q25. As you may be aware, search engines and social networking sites track your internet use in order to do things like target advertising at you. How comfortable are you with (READ OUT) (ROTATE)…?
Is that comfortable or uncomfortable – very of somewhat?

	Very c	Some-what c	Neither	Some-what uc	Very uc	Don't know
Search engines and social networking sites targeting advertising at you based on what you have said and done online	1	2	3	4	5	99
Search engines and social networking sites keeping databases of information on what you have said and done online	1	2	3	4	5	99

Q26. Have you ever put any information on a social networking site that you've later regretted sharing with others?

Yes.....1
No.....2
Have never posted information on a social networking site.....3
Don't know.....99

Q27. Do you think that social networking is …(ROTATE 1 or 2)

Mainly a private activity, where users share information with their friends OR.....1
Mainly a public activity, where users publish information which can be seen by many people.....2
Don't know (DO NOT READ).....99

#OPCQ28.	Thinking now about providing your personal details online. Are you more or less concerned about providing your personal details electronically or online compared to in a hard copy/paper based format?

More 1
Less 2
Same 3
Don't know 99

#OPCQ29.	Are you more or less concerned about the privacy of your personal information while using the internet than you were five years ago?

More 1
Less 2
Same 3
Don't know 99

#OPCQ30.	Do you normally read the privacy policy attached to any internet site?

Yes 1
No 2
Don't know 99

***[If yes, go to Q31]**

#OPCQ31. What impact, if any, did seeing or reading these privacy policies have upon your attitude towards the site? (DO NOT READ) (MULTI)

It's a good idea/ I approve of the privacy policy they are doing the right thing/ prefer to see on sites/ respect sites for having it 1

Feel more confident/ comfortable/ secure/ about using site 2

Appear more honest/ trustworthy/ responsible/ legitimate 3

Helps me decide whether to use the site or not 4

Still apprehensive about sites that have them/ Don't trust them/ not convinced 5

Made me more cautious/ aware when using the internet generally 6

Too long/ complicated to read 7

Other (specify) 8

Don't know 99

[If no to Q 30, ask Q32]

#OPCQ31. Why don't you read website policies? (DO NOT READ)

Too long 1

Hard to find 2

Too complex 3

Agencies and organisations don't comply with them . 4

No need if I trust the organisation 5

Other (specify) 6

PERSONAL ID, THEFT AND FRAUD
I'm going to ask you a series of questions now about how you feel about products or activities that identify you personally, and the possibility of identify fraud and theft.

#OPCQ36.	In which of the following situations, if any, do you think it is acceptable that a COPY or SCAN is made of your identification documents (such as a drivers' license or passport). (MULTI) (ROTATE)

	Acceptable	Not acceptable	Don't know
On entry to licensed premises (e.g. Pub/Club/Hotel)	1	2	99
To obtain a credit card	1	2	99
To purchase general goods (e.g. clothing and food)	1	2	99
To purchase goods for which you need to be over 18	1	2	99
To purchase cigarettes	1	2	99

Q37.	I'd like you to think about the collection and use of your biometric information, which includes fingerprints, pictures of your face or scans of your eyes in a number of different situations? How concerned are you about using biometric information for you to… (ROTATE) Is that very concerned, or somewhat concerned?

	Very concerned	Somewhat concerned	Not concerned	Don't know (DNR)
Get on a flight	1	2	3	4
Do your day to day banking	1	2	3	4
Go into a licensed pub, club, bar or hotel	1	2	3	4
Get into your place of work or study	1	2	3	4

#OPCQ38.	Have you (or someone you personally know) ever been the victim of identity fraud or theft?

Yes – it happened to me.....1

Yes it happened to someone I personally know.....2

No.....3

Don't know.....99

#OPCQ39.	How concerned are you that you may become a victim of identity fraud or theft in the next 12 months? Is that very or somewhat?

Very concerned.....1

Somewhat concerned.....2

Not concerned.....3

Don't know.....99

FINANACIAL CREDIT INFORMATION (CREDIT REPORTING)

I'd like to ask you a few questions now about credit ratings and information that organisations use to work these out. Most people who have rented a house, paid bills for utilities or borrowed money have a credit rating. The information needed to build this rating is available in a credit report.

Q40.	I'm going to read you several statements about credit reports and I'd like you to tell me which is the closest to your understanding of how they work. Do you think that … (READ OUT) (ROTATE)

Everyone is able to see credit information held about them, but they may have to pay a fee to the organisation that holds the information 1

Everyone is able to see credit information held about them and they are able to get this from the organisation free of charge 2

No-one can get access to credit information whether they're prepared to pay for it or not 3

Don't know (DO NOT READ).....99

Q41.	Firstly, have you ever tried to get access to information about your credit rating, this is called your credit report?

Yes 1
No ..... 2 GO TO D1
Don't know ..... 99 GO TO D1

IF YES AT Q41 ASK Q41a

Q41a.	Were you charged for a copy of your credit report?

Yes 1
No 2
Don't know 99

IF YES AT Q41 ASK Q41b

Q41b.	Was information on that credit report correct?

Yes 1
No 2
Don't know 99

IF NO AT Q41b ASK Q41c

Q41c.	Were you able to have the information changed to make it correct?

Yes 1
No 2
Don't know 99

IF NO AT Q41b ASK Q43

Q43. **Have you made a complaint about the fact that there was wrong information on your credit report?**

Yes.....1
No .....2 GO TO D1
Don't know.....99 GO TO D1

IF YES AT Q43 ASK Q44

Q44. **Who did you make this to?**

OPEN

ASK ALL

DEMOGRAPHICS

Thank you. Finally, I just have a few questions about you which we will use simply for the purposes of analysis.

D1 What is the highest level of education you have reached?

Primary school 1
Intermediate (year 10).....2
VCE/HSC (year 12).....3
Undergraduate diploma/TAFE/Trade certs 4
Bachelor's Degree 5
Postgraduate qualification.....6
CAN'T SAY 7

D2. Are you now in paid employment?
IF YES, ASK: Is that FULL-time for 35 hours or more a week, or part-time?
IF NO, ASK: Are you retired or a student?

Yes, Full-time 1
Yes, part time.....2
No, retired 3
No, student.....4
Other non-worker 5
Refused.....6

ASK IF WORKING FULL/PART TIME

D3 **Are you employed by someone else or are you an employer?**

Employee 1
Employer 2
Self-employed/SOHO 3
Both 4
Can't say 5

D4. **What is your (last) occupation?**
(OPEN – code to ANZSCO standard)

D5. **Which describes your household income before tax, best? (An estimate will do)**

Less than $25,000 1
$25-75,000 2
$75 - 100,000 3
Over $100,000 4
Refused (do not read) 5

Closing Statements – All

Thank you very much for your time. Your views count and on behalf of the Office of the Australian Information Commissioner and Wallis social and market research, I'm very glad you made them known. In case you missed it, my name is …... from Wallis. The information you have provided cannot be linked to you personally in any way. The results of this survey will be published later this year. They will be published on the Office of the Australian Information Commissioner's website at www.oaic.gov.au

If you have any queries about this study you can call the Australian Market and Social Research Society's free survey line on 1300 364 832.