

# Privacy and Business

July, 2001

- *Prepared for* –

Office of the Federal Privacy Commissioner  
8/133 Castlereagh Street  
Sydney NSW 2000

- *Prepared by* -

Roy Morgan Research  
232 Sussex Street  
Sydney NSW 2000



and the Australian Taxation Office

---

## Preface

The *Privacy Amendment (Private Sector) Act 2000* is due to commence on 21 December 2001. The purpose of the Office of the Federal Privacy Commissioner (OFPC) is to promote an Australian culture that respects privacy. Our strategic Plan 2000 identifies four key result areas in the lead up to the commencement of the Privacy Amendment (Private Sector) Act. Important among these is gaining a comprehensive understanding of current community (including organisations) attitudes towards privacy. The research will contribute significant input into the networks we are developing with, among others, business organisations, community groups and the health sector. Most immediately the outcomes of this research will inform the Office's communication strategy for the Privacy Amendment (Private Sector) Act.

*Privacy and Business* is among the most comprehensive research of its kind in Australia. It suggests that so far, Australian business has demonstrated a positive attitude to its impending responsibilities. However, this is matched by a low level of understanding about what exactly those responsibilities are. The ramifications of this are potentially serious.

Key trends in today's business world include: Customer Relationship Management, e-Business and e-Commerce; and database mining. In the not-for-profit sector, for example, there is a greater move towards relationship marketing to enhance donor relationships and sustain long term giving. In the health sector, investment in e-health initiatives is growing rapidly. These trends can involve collection of a large volume of detailed, and possibly intimate, personal information. However many businesses pursuing these strategies will be covered by the new Act and may need to adjust the way they handle personal information in order to comply.

Importantly though, compliance with the Act should not be the *sole* concern of business. The OFPC research *Privacy and the Community* illustrates that individuals care about their privacy and these concerns are growing. Organisations, be they on or off line, must attend to the privacy concerns of individuals. As organisations seek increasingly intimate relationships with their customers, relationships that are dependent upon trust, privacy clearly becomes an imperative that no business can afford to ignore.

Finally I would like to thank our Privacy Partners in this project: Australian Information Industry Association; Centrelink; Freehills; and Pricewaterhouse Coopers; and our project sponsor, the Australian Taxation Office. The generous support of these organisations enabled us to take a more thorough look at privacy and the corporate culture in Australia today.

Malcolm Crompton  
Federal Privacy Commissioner  
July 2001



---

## Contents

<b>1. EXECUTIVE SUMMARY.....</b>	<b>1</b>
<b>2. INTRODUCTION.....</b>	<b>17</b>
2.1 Background information.....	17
2.2 Research objectives .....	17
<b>3. METHODOLOGY.....</b>	<b>27</b>
3.1 Interviewing.....	18
3.2 Questionnaire design .....	18
3.2.1 Pilot testing of the questionnaire .....	18
3.3 Sampling frame and sample design .....	19
3.4 Response Rates.....	19
<b>3.5 SAMPLE CHARACTERISTICS.....</b>	<b>20</b>
3.5.1 Size of organisations.....	20
3.5.2 Location of organisations .....	21
3.5.3 Type of industry .....	21
3.5.4 Position of respondents in organisations .....	22
3.5.5 Position of respondents in organisations by type of industry .....	22
3.5.6 Location of privacy officer.....	23
<b>4 MAIN FINDINGS.....</b>	<b>26</b>
4.1 Importance of Privacy of Customers' Personal Information.....	26
4.1.1 Reasons for Importance of Privacy of Customers' Personal Information to Organisation .....	29
4.2 Impact of Breach of Privacy on Public Profile of Organisation.....	33
4.3 Impact of Breach of Privacy on Organisation's Customer Relations.....	37
4.4 Success of Business and Maintaining Customer Privacy .....	40
4.5 Respondents' understanding of the term "Personal Information" .....	44
4.6 Organisational Factors and Customer Trust .....	46
4.7 Customer Service Factors in Dealing with Organisations.....	48
4.8 Privacy Guidelines in Organisations .....	49
4.9 Type of Privacy Guidelines Followed by Organisations.....	53
4.10 Obtaining Information About Customers From Other Organisations .....	55
4.11 Providing Information About Customers To Other Organisations.....	57
4.12 Transfer of Customer Information Within Organisations .....	59
4.13 Concerns About Transfer of Customers' Personal Information .....	60
4.14 Attitudes Toward Use and Protection of Customer Information.....	62
4.15 Awareness and Knowledge of Federal Privacy Laws .....	66
4.16 Organisational Knowledge About New Federal Privacy Laws .....	71
4.17 Impact of New Federal Privacy Laws on Businesses.....	74
4.18 Attitudes to Changes to the Federal Privacy Legislation.....	76
4.19 Reasons for Viewing Changes to Federal Privacy Legislation as Positive .....	77
4.20 Reasons for Viewing Changes to Federal Privacy Legislation as Negative.....	79
4.21 Impact of New Federal Privacy Laws on Consumers .....	80

---

4.22	Internet Privacy Issues Relating to Clients' Personal Information.....	81
4.23	Organisation Websites.....	83
4.24	Protecting Client Privacy On-line.....	84
4.25	Future Impact of New Federal Privacy Laws on Businesses .....	85
4.26	Ways that New Federal Privacy Laws Impact on Businesses .....	86
4.27	Organisational Preparation for New Legislation .....	88
4.28	Sufficiency of Information to Prepare for New Legislation .....	90
4.29	Barriers to Organisational Compliance With New Legislation.....	92
4.30	Sources for Further Information About New Privacy Laws.....	94
4.31	Awareness of the Office of the Federal Privacy Commissioner.....	95
4.32	Assistance From the Office of the Federal Privacy Commissioner to Organisations.....	97

### **List of Tables**

Table 1:	Response Rates for Interviews.....	20
Table 2:	Distribution of Respondents by State/Territory .....	21
Table 3:	Distribution of Respondents by Type of Industry.....	22
Table 4:	Distribution of Respondents by Position in Organisation.....	22
Table 5:	Distribution of Respondents by Position in Organisation and Type of Industry.....	23
Table 6:	Location of Privacy Officer .....	24
Table 7:	Location of Privacy Officer by Type of Industry.....	24
Table 8:	Location of Privacy Officer by State .....	25
Table 9:	Importance of Privacy of Customers' Personal Information .....	26
Table 10:	Importance of Privacy of Customers' Personal Information by Type of Industry.....	27
Table 11:	Importance of Privacy of Customers' Personal Information by Size of Organisation and Location of Privacy Officer.....	28
Table 12:	Importance of Privacy of Customers' Personal Information by State.....	29
Table 13:	Reasons for Privacy of Customers' Personal Information Being Important.....	30
Table 14:	Reasons for Importance of Privacy of Customers' Personal Information by Industry .....	31
Table 15:	Most Common Reasons for Importance of Privacy of Customers' Personal Information by Type of Industry .....	32
Table 16:	Impact of Breach of Customer Privacy to Organisation's Public Profile .....	34
Table 17:	Impact of Breach of Customer Privacy on Organisation's Public Profile by Type of Industry .....	35
Table 18:	Impact of Breach of Customer Privacy on Organisation's Public Profile by Size of Organisation and Location of Privacy Officer.....	36
Table 19:	Impact of Breach of Customer Privacy on Organisation's Public Profile by State .....	37
Table 20:	Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations .....	37
Table 21:	Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations by Type of Industry.....	38

---

Table 22: Impact of Publicity Concerning Breach of Customer Privacy .....	39
Table 23: Impact of Publicity Concerning Breach of Customer Privacy, by State .....	40
Table 24: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information.....	41
Table 25: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by Industry.....	42
Table 26: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by Size of Organisation and Location of Privacy Officer.....	43
Table 27: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by State .....	44
Table 28: Respondents' Definitions of the Term "Personal Information" .....	45
Table 29: Reasons for Customers to Trust Organisation with Personal Information.....	47
Table 30: Factors Believed to be Important to Customers in Choosing to Deal with Organisation .....	48
Table 31: Existence of a Relevant Industry Association for Customer Privacy Issues.....	49
Table 32: Existence of a Relevant Industry Association for Customer Privacy Issues by Type of Industry .....	50
Table 33: Existence of a Relevant Industry Association for Customer Privacy Issues by Size of Organisation and Location of Privacy Officer.....	51
Table 34: Existence of a Relevant Industry Association for Customer Privacy Issues by State.....	52
Table 35: Type of Privacy Guidelines Followed by Organisations .....	53
Table 36: Type of Privacy Guidelines Followed by Organisations by Industry .....	54
Table 37: Extent of Organisation Obtaining Customer Information from Other Organisations .....	55
Table 38: Extent of Organisation Obtaining Customer Information from Other Organisations by Type of Industry .....	56
Table 39: Extent of Organisation Providing Customer Information to Other Organisations.....	57
Table 40: Extent of Organisation Providing Customer Information to Other Organisations by Type of Industry .....	58
Table 41: Extent of Organisation Transferring Customer Information Internally for Use in Other Sections of the Organisation.....	59
Table 42: Extent of Organisation Transferring Customer Information Internally for Use in Other Sections of the Organisation by Type of Industry .....	59
Table 43: Degree of Concern About Transfer of a Customer's Personal Information to Another Business Without the Customer's Knowledge .....	61
Table 44: Concern About Transfer of Customer Information to Another Business Without the Customer's Knowledge, by Type of Industry.....	61
Table 45: Attitudes Toward Use and Protection of Customer Personal Information (Statement 1) .....	63
Table 46: Attitudes Toward Use and Protection of Customer Personal Information (Statement 2) .....	64
Table 47: Attitudes Toward Use and Protection of Customer Personal Information (Statement 3) .....	65
Table 48: Awareness and Knowledge of Federal Privacy Laws (Question 1).....	66
Table 49: Awareness and Knowledge of Federal Privacy Laws (Question 2).....	67
Table 50: Awareness and Knowledge of Federal Privacy Laws (Question 3).....	68
Table 51: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 1).....	70
Table 52: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 2).....	70
Table 53: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 3).....	70

---

---

Table 54: Extent of Organisational Knowledge About New Privacy Laws.....	71
Table 55: Extent of Organisational Knowledge About New Privacy Laws by Type of Industry .....	72
Table 56: Extent of Organisational Knowledge About New Privacy Laws by Size of Organisation and Location of Privacy Officer .....	73
Table 57: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted.....	74
Table 58: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted by Type of Industry .....	75
Table 59: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted by Size of Organisation .....	76
Table 60: Impact of Changes to the Federal Privacy Legislation for the Business Community.....	77
Table 61: Reasons for Viewing Changes to Federal Privacy Legislation as Positive for the Business Community .....	78
Table 62: Reasons for Viewing Changes to Federal Privacy Legislation as Negative for the Business Community.....	79
Table 63: Impact of Changes to the Federal Privacy Legislation for Consumers .....	80
Table 64: Extent of Customer Concerns About Security of Personal Information on the Internet.....	81
Table 65: Extent of Customer Concerns About Security of Personal Information on the Internet by Type of Industry .....	82
Table 66: Existence of Organisation Website .....	83
Table 67: Existence of Organisation Website by Type of Industry .....	84
Table 68: Special Measures Needed to Protect Client Privacy On-line .....	85
Table 69: Extent of Future Impact of New Federal Privacy Laws on the Way Business is Conducted.....	86
Table 70: Ways That New Federal Privacy Laws Will Impact on Business.....	87
Table 71: Organisational Preparation for the New Legislation.....	88
Table 72: Organisational Preparation for the New Legislation by Industry.....	88
Table 73: Organisational Preparation for the New Legislation by Size of Organisation and Location of Privacy Officer.....	89
Table 74: Organisational Preparation for the New Legislation by State.....	90
Table 75: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation .....	91
Table 76: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation by Type of Industry .....	91
Table 77: Potential Barriers to Organisational Compliance with New Legislation .....	93
Table 78: Possible Sources to Contact for Further Information About New Privacy Laws.....	94
Table 79: Awareness of the Office of the Federal Privacy Commissioner .....	95
Table 80: Awareness of the Office of the Federal Privacy Commissioner by Industry .....	96
Table 81: Ways that the Office of the Federal Privacy Commissioner Can Assist Organisations to Prepare for Amended Privacy Laws.....	98

---

## List of Figures

Figure 1: Distribution of Respondents by Position in Organisation.....	23
Figure 2: Location of Privacy Officer.....	25
Figure 3: Importance of Privacy of Customers' Personal Information .....	27
Figure 4: Impact of Breach of Customer Privacy to Organisation's Public Profile .....	35
Figure 5: Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations.....	39
Figure 6: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information.....	42
Figure 7: Existence of a Relevant Industry Association for Customer Privacy Issues .....	51
Figure 8: Type of Privacy Guidelines Followed by Organisations .....	54
Figure 9: Extent of Organisation Obtaining Customer Information from Other Organisations.....	56
Figure 10: Extent of Organisation Providing Customer Information to Other Organisations.....	58
Figure 11: Degree of Concern About Transfer of a Customer's Personal Information to Another Business Without the Customer's Knowledge .....	62
Figure 12: Attitudes Toward Use and Protection of Customer Personal Information (Statement 1).....	63
Figure 13: Attitudes Toward Use and Protection of Customer Personal .....	64
Figure 14: Attitudes Toward Use and Protection of Customer Personal Information (Statement 3).....	65
Figure 15: Awareness and Knowledge of Federal Privacy Laws (Question 1).....	66
Figure 16: Awareness and Knowledge of Federal Privacy Laws (Question 2).....	68
Figure 17: Awareness and Knowledge of Federal Privacy Laws (Question 3).....	69
Figure 18: Extent of Organisational Knowledge About New Privacy Laws .....	73
Figure 19: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted.....	83
Figure 20: Extent of Customer Concerns About Security of Personal Information on the Internet.....	83
Figure 21: Organisational Preparation for the New Legislation .....	89
Figure 22: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation.....	92
Figure 23: Awareness of the Office of the Federal Privacy Commissioner .....	97

## **1. EXECUTIVE SUMMARY**

In order to gain further understanding of attitudes in the business community towards privacy issues and awareness of the new privacy legislation, the Office of the Federal Privacy Commissioner commissioned Roy Morgan Research to conduct a national CATI (Computer Assisted Telephone Interviewing) survey among a representative sample of private sector organisations in Australia. Interviews were conducted in June, 2001, with appropriate persons (mainly senior and middle management level) in 560 organisations covering six major industry sectors. (Note that the organisations included in the survey were those handling information relevant to privacy issues.) This section of the report summarises the general overall findings of the research, followed by a breakdown of the results by type of industry, State, and the location of privacy officers. This section also incorporates information obtained from interviews of business leaders as part of the qualitative stage of the project, and relevant findings from the quantitative study of community attitudes towards privacy.

### **Summary of findings**

#### **Importance of maintaining privacy of customer personal information**

Overall, respondents reported highly positive attitudes toward the privacy of customers' personal information. The overwhelming majority (95%) of respondents said that they considered the privacy of customers' personal information to be a very important or important issue for their organisations. The main reasons (representing 51% of responses) given for the importance of the privacy of customer information were: ethical/moral reasons; compliance with company policy; and maintaining confidentiality of customer information in line with the requirements of the organisation's line of business. Other, less common, reasons (representing 22% of responses) included maintaining the reputation or credibility of the business; consumer confidence; and enhancing customers' expectations of the trustworthiness of the organisation.

The majority (80%) of respondents stated that their business was dependent to a considerable extent upon their ability to protect and responsibly use their customers' personal information. Respondents were cognisant of the negative impact of publicity regarding breaches of customer privacy. Most respondents (over 90%) stated that publicity concerning a breach of customer privacy would be damaging to their organisation's public profile and customer relations.



When participants were asked what was most likely to make customers trust their organisation with their personal information, the most common responses (representing 70% of responses) were centred around the organisation's good track record in keeping information confidential; the organisation's reputation, good name, and length of time in business; and information provided to customers about the organisation's commitment to privacy and specific privacy procedures in place. Less common reasons (representing 13% of responses) were knowledge about the organisation's policies regarding selling or giving away private details, and customer relations practices in building close professional relationships with clients.

It is interesting to note, however, that respondents tended to use widely encompassing definitions of the term "personal information". When asked to define the term, the most common responses (representing 60% of responses) were: address (private/business); phone number (private/business); name; and income details. Other, less common responses (representing 22% of responses) were: age; financial, taxation, credit card information, account details; marriage status; and medical information. It is noteworthy that health case notes, customer service information and personal opinions were not mentioned by respondents as constituting "personal information". Thus, while respondents held quite positive attitudes toward protection of customer personal information, it is not clear that they interpreted the term "personal information" in the same way as the privacy legislation.

These responses from representatives of business sectors to the question of what constitutes personal information are similar to those expressed by respondents in the community survey. The types of personal information people in the community felt reluctant about divulging included financial details, income, health information, and home contact details.

With respect to trusting organisations with their personal information, community respondents were more likely to trust organisations that gave them control over how their personal information was used, and those that had a privacy policy. The results of the business survey suggest acknowledgment of customers' views regarding privacy and a willingness on the part of business to respect privacy of personal information and work towards obtaining and maintaining their customers' trust in the organisation's commitment to privacy.

These findings are also in keeping with comments obtained from interviews with business leaders in the qualitative study:

*They [people] want to feel that they've got control over what's happening with their information. That's something we need to think of as an organisation ...*

---

*ensuring that we meet that expectation test of what our customers expect because it's in our interests not to get that wrong. Because if we consistently get it wrong, we are going to upset a lot of customers. There's no business commercial value in that.*

*If we have a privacy breach, it will be through accident rather than intent. It will be through unconscious act rather than for someone failing to perceive the impact of what they're doing with the information.*

*There is a bit of paranoia around here [about media publicity] because a lot of the reporting of privacy to date has focused very much on the abuse.*

*If history is anything to go on, when there is a privacy breach and it is a high-profile one, there would be heaps of media interest, lots of political interest, and that will then be a big beat-up in the press, which will then play on consumers' minds. So you end up with consumers who become increasingly frightened about these privacy issues, even though generally there may well be very little to be frightened about. That will then in turn effect their take-up of, for example, e-commerce products and also the amount of information they are willing to divulge.*

*The publicity given to non-compliance will effect people's concerns about privacy, which is kind of negative, but at the same time they need to be aware, and then that will effect business. So it will definitely effect us all.*

*I think there have been some fairly high-profile issues about privacy in Australia [recently] where databases have gone missing, credit card details have gone missing, all of that kind of stuff, and every time it happens, there is lots of publicity, and rightly so. I mean if you lose a database or a credit base, that is incredible. Again, it will be just another peak, a high point in the privacy issue and the first breaches start. Then eventually, hopefully, it will kind of die off to [people becoming] more comfortable with the way information is being used.*

### **Use and protection of customer personal information**

In general, respondents tended to hold responsible views about the use and protection of customer personal information. The majority (76%) disagreed with the statement: *"Businesses should be able to use the customer information they collect whenever, and for whatever purpose they choose."* Most (95%) respondents agreed with the statement: *"It is reasonable that there should be laws to protect consumers' personal information held on business databases."* Further, most (86%) respondents agreed with the statement: *"An organisation's customer database is a valuable commercial asset."*

It would appear, then, that most respondents realised the value of customer personal information and recognised that protecting such information was in the interests of the organisation and its relationship with customers.

The majority (64%) of respondents stated that their organisations *never* obtained information about customers or potential customers from other organisations; only 14% of respondents said that they regularly obtained such information from other organisations. Most (90%) respondents said that their organisations *never* sold, rented out, or transferred customer details to other organisations; only 4% said they regularly engaged in transferring such information to other organisations. This is an interesting finding. Given the large amount of marketing materials people receive, it may be that only a small proportion of businesses are engaging in these activities and these businesses would be responsible for a fairly high proportion of such information transactions.

About half the sample (48%) said that their organisations *never* transferred customer details internally for use in relation to different services or products offered by other sections of the company. However, a substantial proportion (a little over 20%) of respondents said their organisations did regularly transfer such information internally. Clearly, these organisations need to have adequate knowledge about the new privacy regulations and implement them accordingly to the internal transfer of information.

Overall, respondents expressed considerable concern about the transfer of customer personal information without the customer's knowledge. Most (90%) respondents said that such actions would be of great concern or some concern to their organisations. The majority (64%) of respondents also noted that when dealing with the Internet, customers would have more concerns about the security of their personal details than usual. About 80% of respondents noted that their organisations had already established a website, and another 10% intended to establish a website. About 55% of these respondents said that their organisations would need to consider special measures such as security protocols, security of data, on-line privacy policies and password protection, in order to protect client privacy on-line.

Business attitudes towards the protection of privacy seem to be compatible with community attitudes. In the community survey, attitudes reflected a strong desire for people to gain control over how their personal information was used, and wanting businesses to seek permission before using their personal information for marketing purposes. Organisational practices that concerned community members, such as transferring personal information without the owner's knowledge, and using personal information beyond the purpose for which it was originally collected, were practices that also concerned representatives of the business community.

An interesting area of contrast, however, was in response to the question of factors that customers consider important in choosing whether or not to deal with a company. In the community survey, respondents rated “*respect for, and protection of, my personal information*” as the most important factor, and over one-third of community respondents rated this service aspect above quality of product, efficiency, price and convenience. In contrast, business respondents rated “*quality of product or service*” as the most important factor. Further, quality of product, efficiency of service, price, and convenience were rated as more important than “*protection or security of personal information*”. Thus, it would appear that businesses are not fully aware of the high importance that the community places on privacy issues with respect to choice in dealing with a particular organisation.

### **Awareness and knowledge of federal privacy laws**

While the majority (82%) of respondents were aware of the existence of federal privacy laws before the interview, there appear to be some gaps in specific knowledge about the legislation. Less than 40% of respondents were aware of what organisations the federal privacy laws applied to. Less than 40% of respondents were aware that new federal privacy laws come into effect in December 2001.

About half (52%) the sample noted that their organisations had very little knowledge or no knowledge at all concerning the new privacy laws. The majority (74%) of respondents stated that their organisations had not started preparing for the new legislation. Further, most (91%) respondents believed that they did not have sufficient information on the new privacy laws to begin preparing for the new legislation.

However, about 40% of respondents noted that there was an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers’ personal information. Of those who had access to relevant industry association guidelines, the majority (60%) of respondents said that their organisations currently followed the privacy guidelines set out by the industry association and 35% said they followed their own guidelines.

Thus, it would seem that industry associations are an avenue through which organisations can obtain relevant information and guidelines for implementation of appropriate privacy procedures. These findings also confirm the appropriateness of the strategy of the Office of the Federal Privacy Commissioner to work actively through industry associations with respect to providing information about the new

---

privacy regulations. The Office is clearly moving in the right direction in this business communication strategy.

### **Impact of new federal privacy laws on business**

About 60% of respondents who were aware of the new privacy laws stated that they would have considerable impact upon the way their business is conducted. The majority (73%) of respondents viewed the changes to the federal privacy legislation as a positive event; only 12% said that the changes were somewhat negative. (Note these questions were directed at those respondents who stated that their organisations had a high level or some knowledge concerning the new federal privacy laws.)

The main reasons for saying the changes to the federal privacy legislation are a positive event (representing 77% of positive responses) were that it would be beneficial to the business and improve customer relations; give consumers more confidence about what information is kept about them in the organisation, and the way such information is kept; lessen the misuse of private information and prevent unauthorised intrusion; and make businesses more honest and ethical. The main reasons for saying the changes to federal privacy legislation are a negative event (representing 76% of negative responses) were that it would be expensive to implement; be too restrictive for businesses; and it would require considerable resources to implement.

When respondents were asked about how the new laws will impact upon their business, a considerable proportion of respondents (17%) said that the new laws would have moderate impact or not much impact, and 6% said that they already partly complied with the new laws. A number of responses to this question (12%) showed positive impact of the new federal privacy laws, with respondents noting that the new laws make businesses more aware of privacy regulations and their responsibility regarding privacy, as well as improving business practice.

The most common responses (55%) showing negative impact of the new laws included: increased work, paperwork and red tape; cost of implementation; requirements for staff training; increased monitoring and control; the need to make new declarations and inform customers to the new laws; and limitations on the amount or type of data that could be collected. Thus, the negative impact of the new laws seems to focus on practical implementation issues, including compliance costs.

When asked about barriers or potential barriers to organisational compliance with the new legislation, the most common responses (23%) were: lack of information; cost

of staff education and training; cost of updating technology systems; and the time taken to implement the new laws, update systems, and reporting to Government.

Comments from interviews conducted with business leaders for the qualitative study complement these findings, showing a mixed reaction to the impact of the new federal privacy laws on business:

*From what we've read so far, we should be all right. Obviously the more we read about it [the legislation], the more we need to think about it, but I think overall we shouldn't be too bad.*

*I think a lot of it's in your head in lots of ways. The move to applying similar principles to the private sector doesn't cause minimum level of disquiet. Some of the other [companies] are going, "This is awful." In reality, once you set the processes in place, it actually works quite smoothly.*

*I think business people are going to look at this as yet another government intervention in their jobs. I absolutely see that.*

*What we will do is obviously put into place a privacy policy which will be an extension to our security policy that's already in place. I think it's [going to be a] challenge to make the transition, the legislative transition, and pick up the bits without creating something everyone has to worry about.*

*[Similar organisations] are concerned about the costs in terms of once you move into a model where you have got some sort of information privacy principles you are bound to do things in a certain way to comply. There are compliance costs, and the idea of compliance is that quite often you do those things because they make good business sense in any event. You don't just do them.*

*I believe in essence the amended Act represents good business sense. The Act is not onerous, the requirements are minimal and by following the National Privacy Principles, we will minimise irritation to the general public, better target our prospects and donors, resulting in more efficient marketing campaigns and better financial results.*

## **The Office of the Federal Privacy Commissioner**

When respondents were asked about who they would contact in order to obtain further information on the new privacy laws, the most common responses (74%) were (in descending order): Industry Association; Privacy Commissioner; Solicitor/Lawyer; and Government Department (State or Federal). Those who did not mention the Office of the Federal Privacy Commissioner as a source of information about the new privacy legislation were asked whether they were aware of the Office before the

---

interview. The majority (64%) of these respondents said they had not been aware of the Office of the Federal Privacy Commissioner.

These findings suggest that while the level of knowledge amongst the business community about the Office is considerably higher than amongst consumers (as expressed in the quantitative Community Survey), there remain a substantial proportion of organisations that need to direct their attention to the resources available to help implement privacy procedures according to the new legislation.

The last question put to respondents who said their organisations had some knowledge of the new privacy legislation concerned the ways that the Office of the Federal Privacy Commissioner could assist their organisations to prepare for the amended privacy laws that come into effect in December, 2001. The majority (72%) of respondents answered this question with the response “more information”. Less common responses (representing 18% of responses) were: training for staff; support to industry associations; simplification of information; and workshops or seminars. Clearly, what respondents want is more information. However, the type of information required has not been specified.

Some comments obtained from business leaders in the qualitative study suggest that privacy issues regarding business-to-business exchange of information are likely to need clarification.

*It's the companies like us that haven't been caught up in this in the past [that need clear guidelines about the new privacy laws]. We have probably been on the periphery, but we didn't know it. For example, we would process information [provided by another company] and our own security steps would be in place. We are not going to sell that information to anybody; we are not going to pass it on to anybody. We have done as instructed by the owners and it's their responsibility to make sure they are doing everything right [by the privacy laws]. If we did something under their instructions that was wrong, I guess somebody could come to us and say, "You breached the Privacy Act" and we would say, "Hold on, I was just following instructions from the owner of the data who should know."*

*The biggest fight that industry has got is perhaps not so much with their customer business interface, but it's their business to business relationships, and who actually owns the data. The privacy legislation is actually going to drive a lot of decisions to be made by who owns the data. Whoever owns it is therefore responsible for making it compliant, and it's a joint ownership, then it's got to be made clear to the customer at the time that it's a joint ownership.*

*I think that the people that really have got the most concerns are the people who have already been tied up in the Act anyway: the credit providers, the*

*banks, the finance, the credit and the health area. They have been there, they are already there. It would seem to me that they are pretty well involved.*

In order to clarify such issues, it would appear that the Office of the Federal Privacy Commissioner will benefit from continuation of the business communication strategy of working through relevant industry associations, which are viewed by respondents as supportive and understanding of concerns specific to the type of industry.

## **INDUSTRY SECTORS**

### **Impact of breach of privacy**

Respondents in the industry sectors Finance/Insurance and Education/Health were most concerned about the impact of a breach of customer privacy on their organisation's public profile and customer relations. Their high level of concern about the negative publicity impact of a breach of customer privacy may relate to their responses to other questions about the importance of the privacy of customers' personal information for their organisations. About 90% of respondents in each of these two industry groups stated that the success of their business was highly dependent on their ability to protect and responsibly use their customers' personal information.

While the majority of respondents in both the Finance/Insurance and Education/Health industry groups noted that ethical/moral reasons, confidentiality and company policy were important reasons for maintaining customer privacy, they also noted that the reputation and credibility of their business as well as consumer confidence were important aspects of maintaining customer privacy. Respondents in these two industry groups were also mindful that their line of business required maintenance of customer privacy as they dealt with confidential information. Respondents in the Finance/Insurance and Education/Health sectors also focused on the issue of trust, stating that their customers expected that the organisation would maintain customer privacy, and they wanted customers to trust the organisation.

In contrast, respondents in the industry sector Retail/Manufacturing were less concerned about the damaging impact of publicity concerning a breach of customer privacy on their organisation's public profile or customer relations. About 40% of respondents in this industry group maintained that the success of their business was relatively independent of their ability to protect and responsibly use their customers' personal information. It is interesting to note that, unlike the other industry groups, respondents in Retail/Manufacturing stated that a primary reason for the importance



of the privacy of customers' personal information for their organisation was to ensure that such information was not misused or made available to their competitors.

Most (about 90%) respondents in the other industry groups (Publishers/Advertisers/Direct Mail, Entertainment/Travel, Business/Personal Services) stated that publicity concerning a breach of customer privacy would be damaging to their organisation's public profile as well as their organisation's customer relations. There was, however, a mixed response pattern in these groups about the relationship between the success of their business and maintenance of the privacy of customers' personal information. The majority (77% to 86%) of respondents in these industry sectors said that the success of their business was dependent on their organisation's ability to protect and responsibly use their customers' personal information, but a substantial proportion (13% to 23%) said the success of their business was relatively independent of maintaining the privacy of customers' personal information.

The primary reasons given by respondents in these industry groups (Publishers/Advertisers/Direct Mail, Entertainment/Travel, Business/Personal Services) for the importance of privacy of customers' personal information related to ethical/moral issues, confidentiality, company policies, and the nature of the information managed by the organisation. In effect, respondents in these industry sectors seem to hold to the notion that privacy of customer information was important because their organisations dealt with confidential information and they must abide by organisational policies.

### **Existence of relevant industry associations**

The Finance/Insurance sector seems to be best served in terms of relevant industry associations. This was the only industry group where the majority (70%) of respondents stated there was an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information. The majority (63%) of respondents in Finance/Insurance organisations that had access to industry association guidelines stated that their organisations currently followed the privacy guidelines set out by the industry association.

The industry sectors that seem to be less well served by industry associations are Retail/Manufacturing and Entertainment/Travel. The majority of respondents in both these industry groups (60% and 70%) said they were not aware of an industry association relevant to their organisations that had developed appropriate privacy protocols for customers' personal information. Of those respondents in Retail/Manufacturing and Entertainment/Travel organisations that had access to

industry association guidelines, about 60% said their organisations currently followed the guidelines set out by the industry association.

The other industry sectors (Publishers/Advertisers/Direct Mail, Business/Personal Services, and Education/Health) showed much variation in terms of access to relevant industry associations. About half the respondents in each of these industry sectors stated that there were no industry association privacy guidelines available to their organisations, about 40% in each of the industry groups said they did have relevant industry association guidelines, and about 10% in each group did not know whether such guidelines were available. However, the majority (about 60%) of those who had access to industry association guidelines in these industry sectors noted that their organisations currently followed the privacy guidelines set out by the relevant industry associations.

### **Transfer of customer information by Industry Sectors**

Type of industry does not seem to effect the extent to which organisations sell, rent out, or transfer customer details to other organisations. The large majority (85% to 96%) of respondents in each of the industry groups stated that their organisations never provided customer information to other organisations.

There was little variation across industry sectors with respect to the degree of concern about the transfer of a customer's personal information to another business without the customer's knowledge. Most (85% to 95%) respondents in each of the industry groups stated that such a situation would be of great concern or some concern to their organisations.

The particular industry sector does not seem to effect the extent to which organisations transfer customer details internally for use in relation to different services or products offered by other sections of the company. About half (41% to 54%) the respondents in each of the industry sectors said their organisations never engaged in internal transfer of information. Roughly the same proportion (43% to 55%) of respondents in each of the industry sectors said their organisations occasionally or regularly transferred customer details internally for use in other sections of the company. These findings suggest that there is a high volume of industries that are likely to have compliance concerns.

There were, however, differences across industry groups in obtaining customer information from other organisations by purchasing, renting, or swapping lists for marketing. According to respondents, the organisations that were occasionally or regularly obtaining information about customers or potential customers from other

organisations tended to be in the industry sectors Publishers/Advertisers/Direct Mail and Retail/Manufacturing. Organisations that seem less likely to obtain customer information occasionally or regularly from other organisations were in the Entertainment/Travel sector. However, a substantial proportion (about 30%) of respondents in each of the industry groups Finance/Insurance, Business/Personal Services and Education/Health noted that their organisations occasionally or regularly obtained customer information from other organisations.

This finding highlights a potential compliance problem. Businesses may believe that purchasing information from another organisation does not require additional compliance procedures on their part. However, there are some industry sectors, such as health, that have particular privacy regulations to consider with respect to use and storage of customer information that are not covered in the privacy policy of the organisation from which they have obtained the information. Such problems are likely to be complex when dealing with business to business exchange of information.

### **Attitudes toward privacy of customer personal information by Industry Sector**

Responses to statements about the use and protection of customer personal information showed little variation across industry sectors. The majority (72% to 80%) of respondents in each of the industry sectors disagreed with the statement that businesses should be able to use the customer information they collect whenever and for whatever purpose they choose.

Most (93% to 99%) respondents in each of the industry sectors agreed with the statement that there should be laws to protect consumers' personal information held on business databases. Similarly, most (83% to 89%) respondents in each of the industry groups agreed with the statement that an organisation's customer database is a valuable commercial asset.

Type of industry does not seem to effect respondents' beliefs about security of personal information on the Internet. The majority (67% to 84%) of respondents in all industry sectors noted that their organisation had already established a website, and a substantial proportion (7% to 15%) said their organisation intended to establish a website. With respect to the question of customer concerns about the security of their personal information on the Internet, a similar pattern of responses appeared across industry groups. Between 60% and 68% percent of respondents in all industry groups stated that there would be more customer concerns about security of personal information on the Internet. However, a considerable proportion (14% to 26%) noted that such concerns would be about the same on the Internet as they are currently in other media.

---

## **Awareness and knowledge of federal privacy laws across Industry Sectors**

Respondents' awareness and knowledge of federal privacy laws does seem to vary according to the industry sector of their organisations. Respondents in the Finance/Insurance sector, compared to other industry sectors, seem to be most knowledgeable about the federal privacy laws. Most (93%) respondents in this industry group said they were aware of the existence of federal privacy laws before the interview, 55 percent said they were aware of what organisations the federal privacy laws applied to, and the majority (70%) in this group said they were aware that new federal privacy laws would come into effect in December of this year. The majority (58%) of respondents in the Finance/Insurance sector also stated that they had been aware of the Office of the Federal Privacy Commissioner prior to the interview.

In contrast, while the majority (73% to 87%) of respondents in each of the other industry groups said they were aware of the existence of federal privacy laws, about a quarter (25% to 27%) of those in the industry sectors Retail/Manufacturing and Entertainment/Travel were not aware of the existence of the federal privacy laws. A substantial proportion (13% to 18%) of respondents in the industry groups Education/Health, Business/Personal Services, and Publishers/Advertisers/Direct Mail, were not aware of the existence of the federal privacy laws before the interview.

The majority (62% to 71%) of respondents in all industry sectors, except Finance/Insurance, stated that they were not aware of what organisations the federal privacy laws applied to. Similarly, the majority (59% to 77%) of respondents in all industry sectors, except Finance/Insurance, said that they were not aware that new federal privacy laws come into effect in December 2001. Further, the majority (61% to 79%) of respondents in all industry sectors, except Finance/Insurance, were not aware of the Office of the Federal Privacy Commissioner.

This pattern of responses was repeated for the question regarding the organisation's level of knowledge about the federal privacy laws. Most (72%) respondents in the Finance/Insurance sector said that their organisation had a high level of knowledge or some knowledge concerning the new privacy laws. In contrast, 50 percent of respondents in the Education/Health sector and 42 percent of respondents in Publishers/Advertisers/Direct Mail said that their organisations had some knowledge about the privacy laws. About 60 percent of respondents in each of the industry sectors Retail/Manufacturing, Entertainment/Travel, and Business/Personal Services said their organisations had very little or no knowledge about the new privacy laws.

These findings suggest that industry sectors that have a history or culture of following professional ethical guidelines regarding privacy and confidentiality are likely to be more aware of the new privacy laws than those sectors that do not have a shared history. Certainly, more knowledge would mean more awareness of the new privacy laws, but the findings also suggest that some industry sectors will find the notion of implementing new privacy procedures less familiar, and perhaps more onerous, than others that have existing policies.

### **Impact of privacy laws on business across industry sectors**

The greater awareness and knowledge about the new federal privacy laws shown by respondents in the Finance/Insurance sector could be related to the perceived impact that the laws will have on business in this sector. The majority (77%) of respondents in the Finance/Insurance group said that the new federal privacy laws currently have considerable impact upon the way their business is conducted; only 22 percent of this group said the new laws would have no impact on the conduct of their business. In contrast, a substantial proportion (37% to 46%) of respondents in all other industry sectors stated that the new laws would not impact at all upon the way their business is currently conducted.

### **Preparation for new legislation across industry sectors**

The Finance/Insurance sector appears to be most prepared, compared to other industry groups, for the new legislation. Over half (54%) the respondents in the Finance/Insurance sector said their organisation had started preparing for the new legislation. In contrast, the majority (57% to 75%) of respondents in each of the other industry sectors stated that their organisations had not yet started preparing for the new privacy legislation.

Interestingly, type of industry does not seem to effect perceptions of the information available to prepare for the new legislation. Most (83% to 95%) respondents in all industry sectors, including Finance/Insurance, who stated that their organisations had not started preparing for the new legislation, also said that they did not have sufficient information on the new privacy laws to begin preparing for the new legislation.

## **STATE LOCATION OF ORGANISATIONS**

While all States and Territories were included in the interview sample, more detailed breakdown of responses by location was restricted to those States that had at least 60 respondents (Victoria, New South Wales, Queensland, Western Australia). The State location of organisations in which respondents worked did not seem to effect

respondents' attitudes toward the importance of the privacy of customers' personal information (all considered such information to be important). Attitudes toward the impact of a breach of customer privacy on the organisation's public profile and customer relations also did not vary across State locations (all considered the publicity impact of a breach of customer privacy would be damaging to their organisation).

There were no noticeable differences between respondents in Victoria and New South Wales in responses to the major questions addressed in the interviews. Respondents in organisations in the larger States, Victoria and New South Wales (compared to those in Queensland and Western Australia) were more likely to say that their organisations had started preparing for the new federal privacy legislation.

Respondents in organisations in Victoria, New South Wales, and Queensland (compared to those in Western Australia) were more likely to say that the success of their business was dependent on their ability to protect and responsibly use their customers' personal information. Respondents in these three States also noted that they had access to an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information.

### **PRIVACY OFFICER PRESENT IN ORGANISATION**

Less than 40% of respondents said that their organisations had a privacy officer, that is, a nominated staff member to oversee privacy issues relating to the collection, transfer, and use of customers' personal information. The results of the research suggest that organisations that were more likely to have privacy officers were: located in Victoria and New South Wales; larger in size (i.e., more than 20 employees); and in the industry sectors Finance/Insurance, Education/Health, and Publishers/Advertisers/Direct Mail. Organisations that were less likely to have privacy officers were in the industry sectors Entertainment/Travel, Retail/Manufacturing, and Business/Personal Services.

The presence or absence of a privacy officer in their organisations did not seem to effect respondents' attitudes toward the importance of the privacy of customers' personal information or the impact of a breach of customer privacy on the organisation's public profile and customer relations.

Respondents in organisations that had a privacy officer (compared to those in organisations that did not have a privacy officer) were more likely to state that the success of their business was dependent on their ability to protect and responsibly use their customers' personal information. Those respondents who stated that their

organisations had a privacy officer were also more likely to have an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information and currently follow the privacy guidelines set out by the industry association.

Respondents in organisations that had privacy officers tended to be more knowledgeable about the federal privacy laws. Compared to respondents in organisations without a privacy officer, those in organisations with a privacy officer tended to be aware of the existence of the federal privacy laws, be aware of what organisations the federal privacy laws applied to, and know that the new federal privacy laws come into effect in December this year. Respondents in organisations with privacy officers also stated that their organisations had a high level of knowledge concerning the new privacy laws and that their organisations had started preparing for the new legislation.

In contrast, respondents in organisations that did not have a privacy officer (compared to those in organisations that did have a privacy officer) tended to lack awareness of the existence of the federal privacy laws, what organisations the laws applied to, and when the laws would come into effect. Respondents in organisations without privacy officers noted that their organisations had very little knowledge concerning the new privacy laws and their organisations had not started preparing for the new legislation.

These findings raise an interesting question of causality: What has led to what? Has lack of organisational knowledge about the new privacy laws led to the absence of a privacy officer in these organisations? Conversely, has the lack of a privacy officer led to lack of organisational knowledge about the new privacy laws? Given the Privacy Amendment Bill comes into effect in December of this year, it would seem important for organisations to nominate a person to start the process of attaining appropriate knowledge and instituting procedures towards the organisation's preparation for the new legislation.

## **2. INTRODUCTION**

### **2.1 Background information**

The Office of the Federal Privacy Commissioner (OFPC) is an independent statutory office responsible for promoting an Australian culture that respects privacy. The Office currently has responsibilities under the Federal Privacy Act 1988 for promoting protection of individuals' personal information.

The responsibilities of the Office, however, will alter substantially in December 2001 when the Privacy Amendment Bill (introduced into Parliament in April 2000) comes into effect. The Privacy Amendment Bill proposes to amend the commonwealth Privacy Act 1988 to extend privacy standards to the private sector, thus requiring private sector organisations to meet specified standards for the handling of personal information.

In order to assist in the development of an effective communication strategy to advise the various target groups of the changes, and to inform future policy development, in January 2001, the Office of the Federal Privacy Commissioner commissioned Roy Morgan Research to undertake research into community, business and government agency attitudes toward privacy.

In order to ascertain the views of each target group (i.e., community, business and government) three separate surveys were conducted, each involving a qualitative and quantitative component. For the 'business' target group (the focus of this report), the research included a qualitative component involving face-to-face interviews with senior level management persons in private sector organisations in Sydney and Melbourne. This stage of the research informed the development of the quantitative survey consisting of 560 telephone interviews.

### **2.2 Research objectives**

Broadly, the objectives of the survey involved:

- identifying current practices of organisations in relation to the privacy of personal information;
- identifying business attitudes in relation to privacy issues and practices;
- gauging current levels of knowledge in organisations with regard to privacy; and
- gauging current levels of awareness and understanding of the new privacy laws and the Privacy Commissioner.



### **3. METHODOLOGY**

#### **3.1 Interviewing**

Interviews were conducted with a total of 560 business respondents using a Computer Assisted Telephone Interviewing (CATI) methodology.

In order to ensure interviews were conducted with the most appropriate person in the organisation, the introduction of the questionnaire asked for “the person best able to answer questions on the organisation’s practices concerning the handling of customer personal information”, and provided some examples of the likely position this person might hold. The introduction also contained a screening question to ensure interviews were only conducted with organisations that in some way dealt with consumers’ personal information.

The telephone number that Roy Morgan Research used to contact the organisation was, in most cases, that of the CEO or their PA (rather than the receptionist), hence, the suitability of the organisation for inclusion in the survey and the most appropriate person to respond to the questions could be identified relatively efficiently. Once identified, the respondent was given the option of completing the interview at that time, or could make an appointment for the interviewer to call back.

#### **3.2 Questionnaire design**

The questionnaire was designed in close consultation with staff from the Office of the Federal Privacy Commissioner who, in turn, sought input from a committee of relevant stakeholders. Questionnaire design was aided by the findings from the qualitative phase of the research in terms of identifying appropriate pre-codes to questions and the suitability of the proposed content. The final questionnaire consisted of 46 questions and took just under 20 minutes (19.5) to complete.

##### **3.2.1 Pilot testing of the questionnaire**

In order to ensure the introduction was effective in terms of delivering the most appropriate respondent, and that the questions flowed and were understood by respondents, a pilot of 15 interviews was conducted. Feedback from interviewers revealed that the introduction and questions worked well, hence no changes were made to the questionnaire on completion of the pilot.

A copy of the survey questionnaire is attached at Appendix A.

### **3.3 Sampling frame and sample design**

Contact lists purchased from Dunn and Bradstreet provided the sampling frame for this project. The industry classification system used by Dunn and Bradstreet was the Standard Industrial Classification (US SIC).

The 5,000 individual businesses included in the list were randomly selected from 68 specific industry groups identified by the Office of the Federal Privacy Commissioner. In order to manage industry quotas and reporting, the 68 industries were classified into the following six broad industry groups:

- Publishers/Advertisers/Direct Mail
- Retail/Manufacturing
- Entertainment/Travel
- Finance/Insurance Services
- Business/Personal Services
- Education/Health Services

The type of industries allocated to each of the groups can be seen in Attachment B.

The sample of 500 was allocated evenly across the six broad industry group and quota placed on particular industries within these broad categories to ensure an adequate number of interviews were conducted with organisations of high interest to the Office of the Federal Privacy Commissioner. In order to achieve the quotas and to complete all interviews where appointments had been made, the total number of interviews exceeded the target of 500, and totalled 560.

### **3.4 Response Rates**

The following table shows the number of calls made to achieve the 560 interviews, along with the number of refusals and terminations. Overall, approximately 65% of businesses who were contacted and 'in scope' (i.e., the organisation met the criteria and the best respondent was available) participated in the survey. Of all businesses contacted, that is, those 'in scope' or 'out of scope', 40% participated in the survey.

**Table 1: Response Rates for Interviews**

<b>Response</b>	<b>Number</b>
Used sample	3,745
Interviews achieved	560
Organisation does not fit description	141
Person best placed to answer questions not available	304
Refusals	227
Terminated mid-interview (respondent drop out)	65
Quota fail	2,228
No reply (on last call)	21
Engaged (on last call)	9
Unobtainable (number invalid)	114
Appointments	75

Of those who refused to participate in the interview (n=227):

- 61% said they were too busy;
- 17% said they were not interested;
- 11% thought it was not relevant to their business;
- 3% did not do surveys as part of company policy;
- 1% said their organisation was too small;
- 7% gave other reasons (including unwilling to give information over the telephone, concerns about confidentiality, and needing to get the permission of the manager).

### **3.5 SAMPLE**

#### **3.5.1 Size of organisations**

Slightly more than half the sample (56%, n=315) represented organisations with less than 20 employees; the remainder (44%, n=245) represented organisations with more than 20 employees.

While small businesses (less than 20 employees) account for approximately 96% of all registered businesses in Australia<sup>1</sup>, larger businesses (those with 20 employees or more) were over-sampled in order to maximise the range of views from this important sub-group.

---

<sup>1</sup> ABS figures, 1998/99

While only those organisations (large and small) who handled personal information were included in the research, large businesses were seen as important to the study as the majority will be covered by the legislation, and the impact of the change, in terms of staff training and systems preparation etc., is likely to be relatively significant for this group. Alternatively, not all small businesses will be covered by the legislation as some of them will be able to claim the ‘small business exception’. The responses of small business, nevertheless, were important to the study as the prevalence of this group necessitates a comprehensive understanding of their views and attitudes towards privacy issues.

Furthermore, as a group, small businesses are more difficult to communicate with and obtain direct feedback from, hence the survey provided an ideal opportunity to glean an insight into their views and needs regarding privacy.

### 3.5.2 Location of organisations

The location of participants by State/Territory is shown in Table 2.

**Table 2: Distribution of Respondents by State/Territory**

Location	Total (560) %
New South Wales	34
Victoria	29
Queensland	13
Western Australia	11
South Australia	7
Tasmania	3
Australian Capital Territory	2
Northern Territory	1
Total	100

*Base: All respondents.*

Over half the respondents (63%) were located in New South Wales and Victoria, 31% were located in Queensland, Western Australia, and South Australia, and the remaining 6% were located in Tasmania, the ACT and Northern Territory.

### 3.5.3 Type of industry

Table 3 shows the distribution of respondents in each of the six industry groups.

**Table 3: Distribution of Respondents by Type of Industry**

Type of Industry	Total (560) %
Publishers/ Advertisers/ Direct Mail	16
Retail/Manufacturing	24
Entertainment/Travel	13
Finance/Insurance	15
Business/Personal Services	15
Education/Health	17
Total	100

About a quarter of the sample (24%) was in Retail/Manufacturing industries. The remainder of the sample was distributed about evenly in the other five categories, ranging from 13% to 17% in each industry group.

#### **3.5.4 Position of respondents in organisations**

The managerial positions of respondents in their organisations are shown in Table 4.

**Table 4: Distribution of Respondents by Position in Organisation**

Position within Organisation	Total (560) %
Senior Management	60
Mid-Level Management	29
Lower Level Management	5
Supervisory	3
Support Staff/Junior Level	3
Total	100

The majority of respondents (60%) were in Senior Management positions (Director/ CEO/ Top Level) within their organisations, about 30% were in Mid-Level Management positions, and the remaining 10% were in Lower Level positions (Lower Level Management/ Supervisory/ Support Staff/ Junior Level).

#### **3.5.5 Position of respondents in organisations by type of industry**

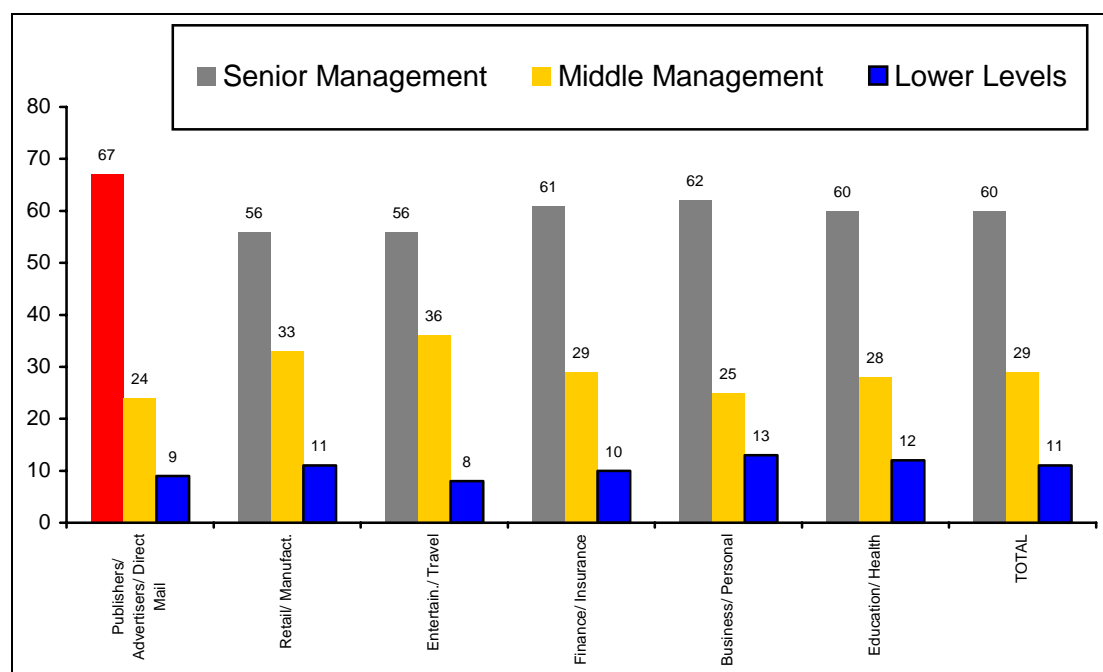
The pattern of distribution of respondents' positions in organisations was consistent across industry groups (see Table 5 and Figure 1).

**Table 5. Distribution of Respondents by Position and Industry**

Position within Organisation	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Senior Management	67	56	56	61	62	60
Mid-Level Management	24	33	36	29	25	28
Lower Level/ Supervisory/ Support Staff/ Junior Level	9	11	8	10	13	12
Total	100	100	100	100	100	100

Base: All respondents.

The majority of respondents in each industry group were in Senior Management (range 56% to 67%) or Middle Management (range 24% to 36%) positions within their organisations.

**Figure 1: Distribution of Respondents by Position in Organisation**

### 3.5.6 Privacy officer in organisation

Respondents were asked, *Does your organisation have a nominated staff member to oversee privacy issues relating to the collection, transfer and use of customers' personal information?* Responses to this question are shown in Table 6 and Table 7.

**Table 6: Location of Privacy Officer**

“Does your organisation have a nominated staff member to oversee privacy issues relating to the collection, transfer and use of customers’ personal information?”

Response	Total % (560)
YES – Organisation has a Privacy Officer	36
NO – Organisation does not have a Privacy Officer	60
Can’t say	4
Total	100

Base: All respondents.

The majority of the sample (60%) noted that their organisations did *not* have a designated privacy officer, and 36% of the sample said they *did* have a privacy officer.

**Table 7: Location of Privacy Officer by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business / Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
YES – Organisation has a Privacy Officer	40	28	32	54	23	40
NO – Organisation does not have a Privacy Officer	52	68	66	41	76	57
Can’t say	8	4	2	5	1	3
Total	100	100	100	100	100	100

Base: All respondents.

The majority of organisations within the different industry sectors (range 52% to 76%, except Finance/Insurance, 42%) did *not* have a nominated staff member to oversee privacy issues. The exception to this pattern is in the Finance/Insurance sector, where 54% of respondents in this group said they *did* have a designated privacy officer in their organisations (see Figure 2).

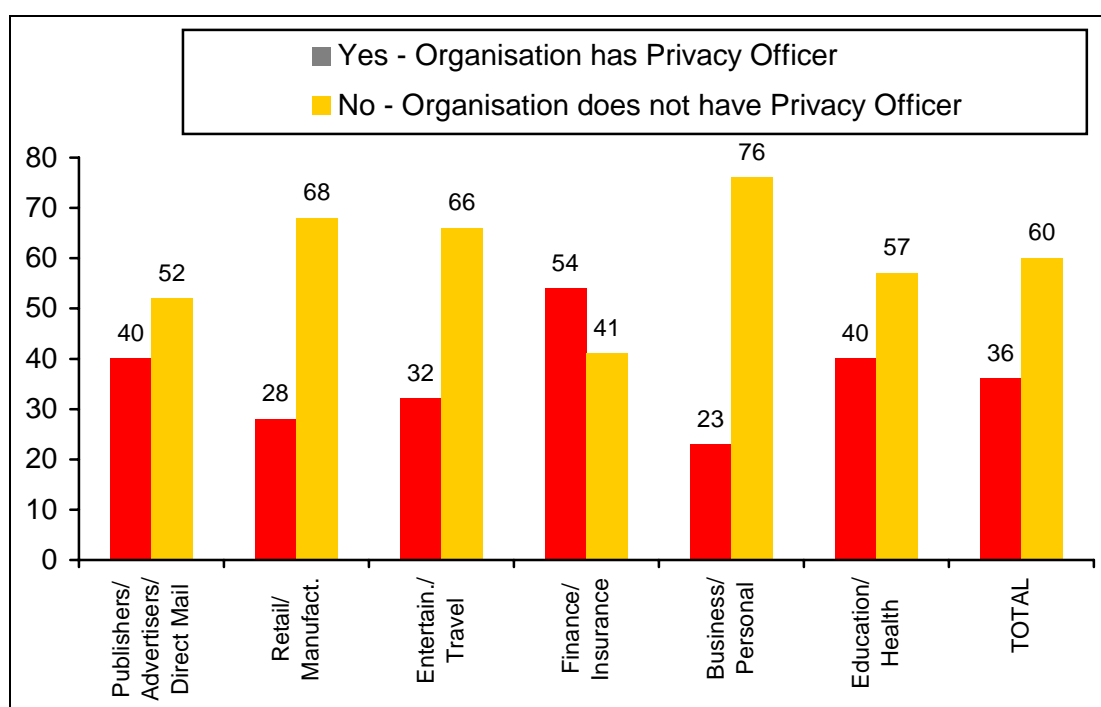
**Figure 2: Location of Privacy Officer**

Table 8 shows responses to the question about designated privacy officers by State location. (Note that data only from those States with more than 60 respondents interviewed are shown in the table.)

**Table 8: Location of Privacy Officer by State**

Response	VIC (164) %	NSW (188) %	QLD (74) %	WA (61) %
YES – Organisation has a Privacy Officer	38	38	26	28
NO – Organisation does not have a Privacy Officer	55	58	73	69
Can't say	7	4	1	3
Total	100	100	100	100

Base: All respondents in specified States.

The majority (55% to 73%) of respondents in the four States said that their organisations did not have a privacy officer. Victoria and New South Wales seem better served with respect to privacy officers than Queensland and Western Australia. About 40% of respondents in Victoria and in New South Wales said they had privacy officers in their organisations.



## 4 MAIN FINDINGS

### 4.1 Importance of Privacy of Customers' Personal Information

Responses to the question, *How important an issue would you consider the privacy of customers' personal information to be for your organisation?* are shown in Table 9.

**Table 9: Importance of Privacy of Customers' Personal Information**

*"How important an issue would you consider the privacy of customers' personal information to be for your organisation?"*

Response	Total (560) %
Very important	84
Important	11
Neither important nor unimportant	2
Not very important	2
Not at all important	0.5
Can't say	0.5
Total	100

*Base: All respondents.*

A large majority of the sample (95%) said they considered the privacy of customers' personal information to be important (*Very important/ Important*); only 3% said it was *not* important (*Not very important/ Not at all important*).

The pattern of responses to the question about the importance of privacy to the organisation was consistent across industry groups (see Table 10).

**Table 10: Importance of Privacy of Customers' Personal Information by Type of Industry**

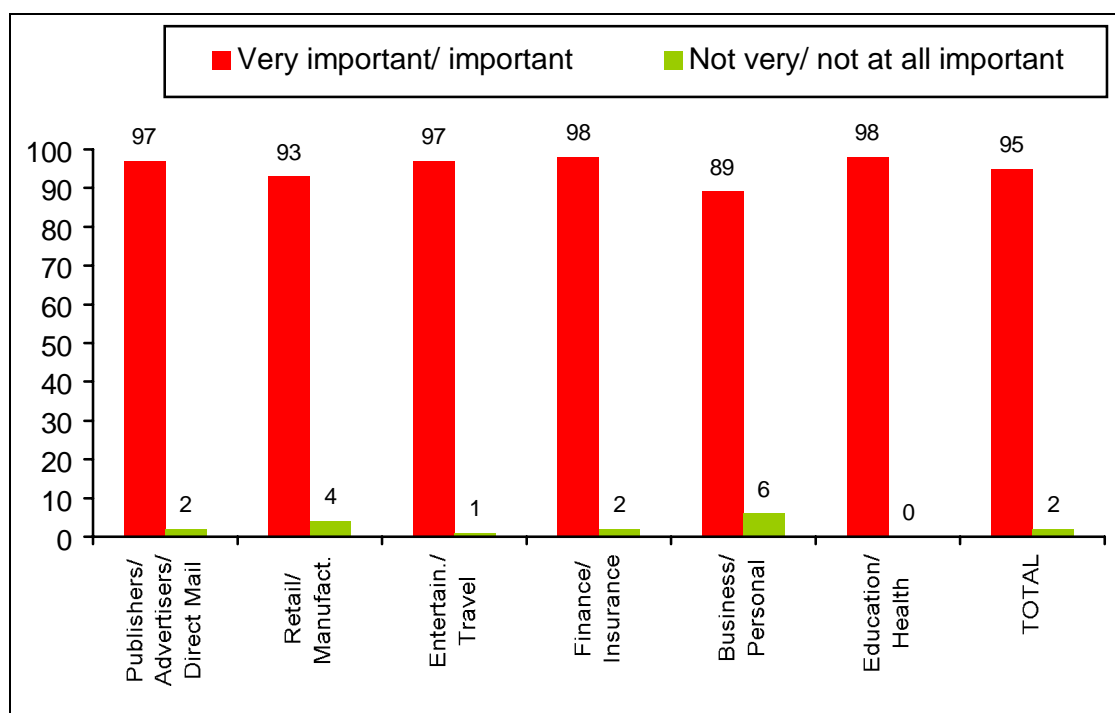
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business / Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Very important/ Important	97	93	97	98	89	98
Neither important nor unimportant	1	2	2	0	4	1
Not very important/ Not at all important	2	4	1	2	6	0
Can't say	0	1	0	0	1	1
Total	100	100	100	100	100	100

*Base: All respondents.*

The large majority of respondents in each industry group (range 89% to 98%) said they considered the privacy of customers' personal information to be important (*Very important/ Important*). Less than 10% in each industry group (range 0 to 6%) said it was *not* important (*Not very important/ Not at all important*) (see Figure 3).

**Figure 3: Importance of Privacy of Customers' Personal Information**

*"How important an issue would you consider the privacy of customers' personal information to be for your organisation?"*



Attitudes toward the importance of the privacy of customers' personal information do not seem to vary by the size of the organisation or whether the organisation has a privacy officer (see Table 11).

**Table 11: Importance of Privacy of Customers' Personal Information by Size of Organisation and Location of Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
Very important/ Important	96	94	97	94
Neither important nor unimportant	1	2	1	2
Not very important/ Not at all important	3	3	2	3
Can't say	0	1	0	1
Total	100	100	100	100

Base: All respondents.

Most respondents (96%) in organisations with less than 20 employees said privacy of customers' personal information was important (*Very important/ Important*), as did most respondents (94%) in organisations with more than 20 employees.

The majority (97%) of respondents in organisations with a designated privacy officer as well as the majority (94%) of those in organisations without a privacy officer said that privacy of customers' personal information was important (*Very important/ Important*).

Attitudes toward the importance of the privacy of customers' personal information do not seem to vary by State location of the organisation (see Table 12).

**Table 12: Importance of Privacy of Customers' Personal Information by State**

Response	VIC	NSW	QLD	WA
	(164) %	(188) %	(74) %	(61) %
Very important/ Important	97	96	97	87
Neither important nor unimportant	1	2	1	2
Not very important/ Not at all important	2	2	2	8
Can't say	0	0	0	3
Total	100	100	100	100

*Base: All respondents in specified States.*

#### **4.1.1 Reasons for Importance of Privacy of Customers' Personal Information to Organisation**

Respondents were asked, *What makes the privacy of customers' personal information an important issue for your organisation?* Responses to this question were coded into eight categories (see Table 13).

**Table 13: Reasons for Privacy of Customers' Personal Information Being Important to Organisation**

*“What makes the privacy of customers' personal information an important issue for your organisation?”*

CODE	Main Reasons	Total (656) %
a	Ethical/moral reasons/ Confidentiality/ It's our policy	30
b	Our line of business requires it/ We deal with confidential information	21
c	Reputation/ Credibility of our business/ Consumer confidence	11
d	Customers expect it of us/ We want customers to trust us	11
e	We handle tax/financial/legal information	9
f	Don't want competition to have this information/ Don't want it misused	6
g	Because of legal implications/ It's the law/ Don't want to get sued	4
h	It is important (essential) for any business/ Is good business practice	2
	Other	4
	Can't say	2
	Total	100

*Note:* Respondents could give more than one reason.

The most common reasons (representing over 10% of responses in each category) given for the privacy of customers' personal information being important were:

- *Ethical/moral reasons/ Confidentiality/ It's our policy*
- *Our line of business requires it/ We deal with confidential information*
- *Reputation/ Credibility of our business/ Consumer confidence*
- *Customers expect it of us/ We want customers to trust us*

Less commonly cited reasons (representing less than 10% of responses in each category) for the privacy of customers' personal information being important were:

- *We handle tax/financial/legal information*
- *Don't want competition to have this information/ Don't want it misused*
- *Because of legal implications/ It's the law/ Don't want to get sued*
- *It is important (essential) for any business/ Is good business practice*

Responses to the question of reasons for the importance of privacy of customers' personal information by industry group are shown in Table 14.

**Table 14: Reasons for Importance of Privacy of Customers' Personal Information by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
a	35	34	36	23	24	26
b	18	15	25	15	24	29
c	15	12	9	11	3	15
d	7	12	10	10	9	16
e	2	3	4	21	23	4
f	6	15	4	6	1	1
g	2	1	4	7	7	5
h	8	1	0	2	3	0
Other	0	4	4	4	5	3
Can't say	0	3	4	1	1	1
Total	100	100	100	100	100	100

Note: See Table 13 for responses corresponding to codes.

The most frequently cited reasons (representing 15% to 36% of responses in each industry group) were:

- *Ethical/moral reasons/ confidentiality/ it's our policy*
- *Our line of business requires it/ We deal with confidential information*

The least frequently cited reasons (representing less than 10% of responses in each industry group) were:

- *Because of legal implications/ It's the law/ Don't want to get sued*
- *It is important (essential) for any business/ Is good business practice*

There are some differences in the pattern of responses across industry sectors to the question, *What makes the privacy of customers' personal information an important issue for your organisation?* These patterns are shown in Table 15 in order of the five most common reasons (i.e., above 10% of responses) given in each industry group.

**Table 15: Most Common Reasons for Importance of Privacy of Customers' Personal Information by Type of Industry**

Order		Publishers/Advertisers/Direct Mail	(92) %
1	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	35
2	b.	Our line of business requires it/ We deal with confidential information	18
3	c.	Reputation/ Credibility of our business/ Consumer confidence	15
Order		Retail/Manufacturing	(135) %
1	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	34
2	b.	Our line of business requires it/ We deal with confidential information	15
3	f.	Don't want competition to have this information/ Don't want it misused	15
4	c.	Reputation/ Credibility of our business/ Consumer confidence	12
5	d.	Customers expect it of us/ We want customers to trust us	12
Order		Entertainment/Travel	(73) %
1	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	36
2	b.	Our line of business requires it/ We deal with confidential information	25
3	d.	Customers expect it of us/ We want customers to trust us	10
Order		Finance/Insurance	(82) %
1	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	23
2	e.	We handle tax/ Financial/ Legal information	21
3	b.	Our line of business requires it/ We deal with confidential information	15
4	c.	Reputation/ Credibility of our business/ Consumer confidence	11
5	d.	Customers expect it of us/ We want customers to trust us	10
Order		Business/Personal Services	(84) %
1	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	24
2	b.	Our line of business requires it/ We deal with confidential information	24
3	e.	We handle tax/ Financial/ Legal information	23
Order		Education/Health	(94) %
1	b.	Our line of business requires it/ We deal with confidential information	26
2	a.	Ethical/moral reasons/ Confidentiality/ It's our policy	29
3	d.	Customers expect it of us/ We want customers to trust us	16
4	c.	Reputation/ Credibility of our business/ Consumer confidence	15

The primary reasons given by all industry groups for the importance of the privacy of customers' personal information concerned confidentiality and business policy:

- *Ethical/moral reasons/ Confidentiality/ It's our policy;*
- *Our line of business requires it/ We deal with confidential information.*

Respondents in Finance/Insurance and Business/Personal Services stated that their primary reasons had to do with confidentiality and business policy, but they also noted that privacy was important because of the nature of the information they managed in their organisations:

- *We handle tax/financial/legal information.*

The reputation of their businesses and wanting the trust of their customers were also common reasons given by most industry groups for the importance of privacy of customers' personal information:

- *Reputation/ Credibility of our business/ Consumer confidence;*
- *Customers expect it of us/ We want customers to trust us.*

Respondents in the Retail/Manufacturing sector were also concerned about the misuse of customers' personal information:

- *Don't want competition to have this information/ Don't want it misused.*

#### **4.2 Impact of Breach of Privacy on Public Profile of Organisation**

Respondents were asked to indicate the publicity impact of a breach of customer privacy to their organisations: *How damaging could publicity concerning a breach of customer privacy be to your organisation's public profile?* The distribution of responses to this question is shown in Table 16.



**Table 16: Impact of Breach of Customer Privacy on Organisation's Public Profile**

*“How damaging could publicity concerning a breach of customer privacy be to your organisation's public profile?”*

<b>Response</b>	<b>Total (560) %</b>
Extremely damaging	63
Somewhat damaging	27
Neither damaging nor not damaging	4
Not very damaging	3
Not at all damaging	2
Can't say	1
Total	100

*Base: All respondents.*

A large majority of respondents (90%) said they thought publicity concerning a breach of customer privacy would be damaging to their organisation's public profile (*Extremely damaging/ Somewhat damaging*); only 5% said it would *not* be damaging (*Not very damaging/ Not at all damaging*).

The pattern of responses to the question about the impact of a breach of customer privacy on the public profile of the organisation was consistent across industry groups (see Table 17).

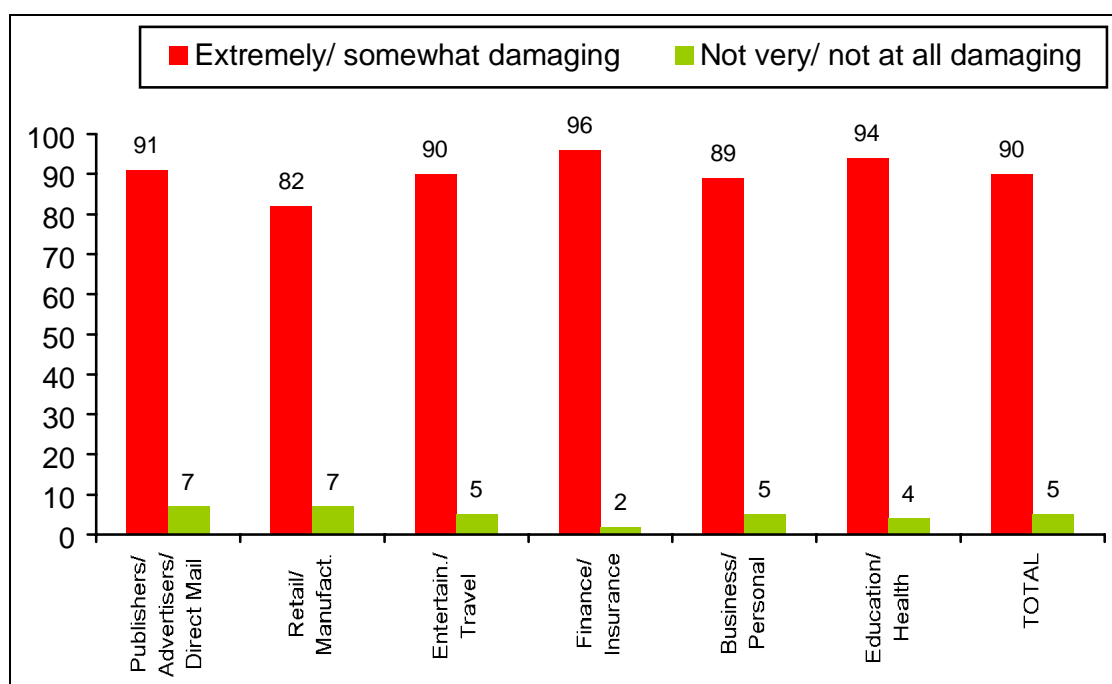
**Table 17: Impact of Breach of Customer Privacy on Organisation's Public Profile by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Extremely damaging/ Somewhat damaging	91	82	90	96	89	94
Neither damaging nor not damaging	2	9	3	1	4	1
Not very damaging/ Not at all damaging	7	7	5	2	5	4
Can't say	0	2	2	1	2	1
Total	100	100	100	100	100	100

Base: All respondents.

The large majority of respondents in each industry group (range 82% to 96%) said they considered publicity concerning a breach of customer privacy would be damaging to their organisation's public profile (*Extremely damaging/ Somewhat damaging*). Less than 10% (range 2% to 7%) said such publicity would *not* be damaging to their organisation's public profile (*Not very damaging/ Not at all damaging*) (see Figure 4).

**Figure 4: Impact of Customer Privacy Breach to Organisation's Public Profile**



Beliefs about the publicity impact of a breach of customer privacy do not seem to vary by the size of the organisation or whether the organisation has a privacy officer (see Table 18).

**Table 18: Impact of Breach of Customer Privacy on Organisation's Public Profile by Size of Organisation and Location of Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
Extremely damaging/ Somewhat damaging	89	91	92	88
Neither damaging nor not damaging	3	4	3	4
Not very damaging/ Not at all damaging	6	4	4	6
Can't say	2	1	1	2
Total	100	100	100	100

*Base: All respondents.*

Most respondents (89%) in organisations with less than 20 employees said such publicity would be damaging (*Extremely damaging/ Somewhat damaging*), as did most respondents (91%) in organisations with more than 20 employees.

The majority (92%) of respondents in organisations with a privacy officer as well as the majority (88%) of respondents in organisations without a privacy officer said that publicity about a breach of customer privacy would be damaging (*Extremely damaging/ Somewhat damaging*).

The pattern of responses to the question about the impact of a breach of customer privacy on the public profile of the organisation was consistent across State locations of organisations (see Table 19).

**Table 19: Impact of Breach of Customer Privacy on Organisation's Public Profile by State**

Response	VIC (164) %	NSW (188) %	QLD (74) %	WA (61) %
Extremely damaging/ Somewhat damaging	90	89	91	89
Neither damaging nor not damaging	5	2	5	3
Not very damaging/ Not at all damaging	3	7	4	7
Can't say	2	2	0	1
Total	100	100	100	100

*Base: All respondents in specified States.*

#### **4.3 Impact of Breach of Privacy on Organisation's Customer Relations**

Responses to the question, *How damaging could publicity concerning a breach of customer privacy be to your organisation's customer relations?* are shown in Table 20.

**Table 20: Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations**

*"How damaging could publicity concerning a breach of customer privacy be to your organisation's customer relations?"*

Response	Total (560) %
Extremely damaging	68
Somewhat damaging	25
Neither damaging nor not damaging	2
Not very damaging	2
Not at all damaging	2
Can't say	1
Total	100

*Base: All respondents.*

Most respondents (93%) said they thought publicity concerning a breach of customer privacy would be damaging to their organisation's customer relations (*Extremely damaging/ Somewhat damaging*); only 4% said it would not be damaging (*Not very damaging/ Not at all damaging*).

The pattern of responses to the question about the publicity impact of a breach of privacy was consistent across type of industry (see Table 21).

**Table 21: Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations by Type of Industry**

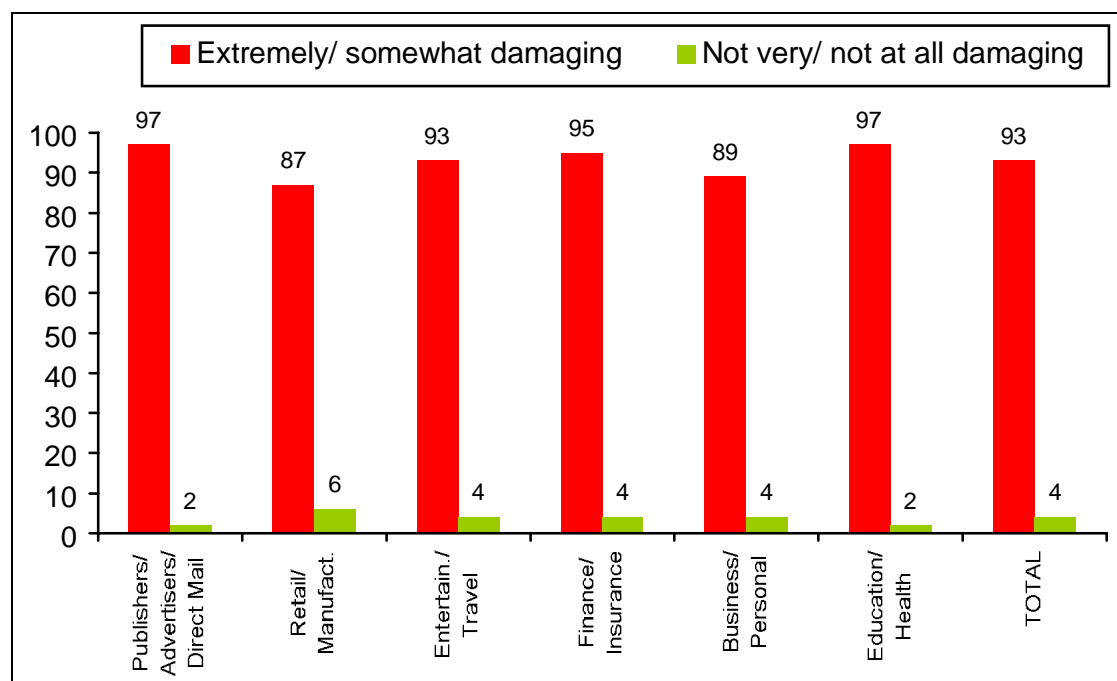
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Extremely damaging/ Somewhat damaging	97	87	93	95	89	97
Neither damaging nor not damaging	0	7	1	0	2	0
Not very damaging/ Not at all damaging	2	6	4	4	4	2
Can't say	1	0	2	1	5	1
Total	100	100	100	100	100	100

*Base: All respondents.*

The majority of respondents in each industry group (range 87% to 97%) said they considered publicity concerning a breach of customer privacy would be damaging to their organisation's customer relations (*Extremely damaging/ Somewhat damaging*). Less than 10% (range 2% to 6%) said such publicity would *not* be damaging to their organisation's customer relations (*Not very damaging/ Not at all damaging*) (see Figure 5).

**Figure 5: Impact of Publicity Concerning Breach of Customer Privacy on Organisation's Customer Relations**

*“How damaging could publicity concerning a breach of customer privacy be to your organisation's customer relations?”*



Beliefs about the possible damage of publicity about a breach of customer privacy on customer relations do not seem to vary by the size of the organisation or whether the organisation had a designated privacy officer (see Table 22).

**Table 22: Impact of Publicity Concerning Breach of Customer Privacy to Organisation's Customer Relations by Size of Organisation and Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees (315) %	≥ 20 Employees (245) %	Has Privacy Officer (199) %	No Privacy Officer (361) %
Extremely/ somewhat damaging	92	93	94	92
Neither damaging nor not	2	3	3	2
Not very /not at all damaging	5	2	2	5
Can't say	1	2	1	1
Total	100	100	100	100

Base: All respondents.

The majority of respondents (92%) in organisations with less than 20 employees said such publicity would be damaging to the organisation's customer relations (*Extremely damaging/ Somewhat damaging*), as did the majority of respondents (93%) in organisations with more than 20 employees.

Most respondents (94%) in organisations with a designated privacy officer as well as most respondents (92%) in organisations without a privacy officer said that publicity about a breach of customer privacy would be damaging to their organisation's customer relations (*Extremely damaging/ Somewhat damaging*).

Beliefs about the possible damage of publicity about a breach of customer privacy on customer relations do not seem to vary by State location of the organisation (see Table 23).

**Table 23: Impact of Publicity Concerning Breach of Customer Privacy to Organisation's Customer Relations by State**

Response	VIC (164) %	NSW (188) %	QLD (74) %	WA (61) %
Extremely damaging/ Somewhat damaging	92	91	95	93
Neither damaging nor not damaging	3	2	3	2
Not very damaging/ Not at all damaging	3	6	1	3
Can't say	2	1	1	2
Total	100	100	100	100

*Base: All respondents in specified States.*

#### **4.4 Success of Business and Maintaining Customer Privacy**

Responses to the question, *To what extent is the success of your business dependent upon your ability to protect and responsibly use your customers' personal information?* are shown in Table 24.

**Table 24: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information**

*"To what extent is the success of your business dependent upon your ability to protect and responsibly use your customers' personal information?"*

Response	Total % (560)
Highly dependent	51
Somewhat dependent	29
Neither dependent nor independent	7
Not very dependent	9
Not at all dependent	3
Can't say	1
Total	100

*Base: All respondents.*

The majority of respondents (80%) said they considered the success of their business to be dependent on their ability to responsibly manage the privacy of their customers' personal information (*Highly dependent/ Somewhat dependent*). However, 12% said the success of their business was *not* dependent on their management of customers' privacy (*Not very dependent/ Not at all dependent*). Differences in responses to this question across industry groups can be seen in Table 25.



**Table 25: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by Industry**

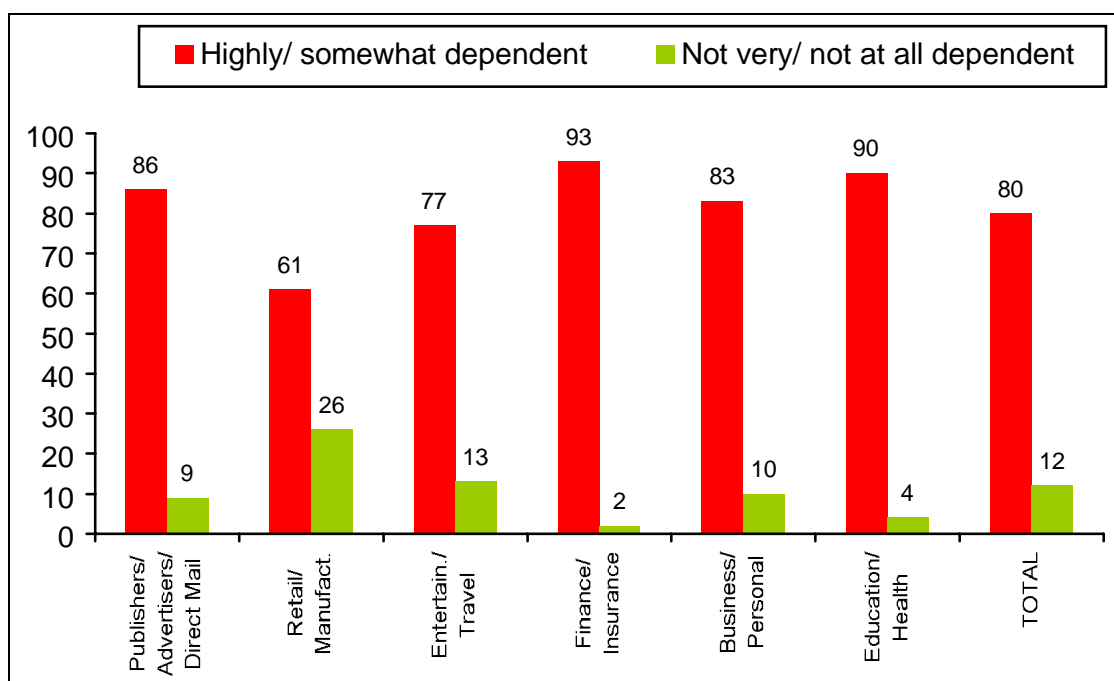
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Highly dependent/ Somewhat dependent	86	61	77	93	83	90
Neither dependent nor independent	4	11	10	4	6	5
Not very dependent/ Not at all dependent	9	26	13	2	10	4
Can't say	1	2	0	1	1	1
Total	100	100	100	100	100	100

Base: All respondents.

The majority of respondents in each industry group (range 61% to 93%) said that the success of their business *was* dependent upon their ability to protect and responsibly use their customers' personal information (*Highly dependent/ Somewhat dependent*). However, a substantial proportion of respondents in two industry groups, Retail/Manufacturing (26%) and Entertainment/Travel (13%), viewed the success of their business to be relatively *independent* of their ability to protect and responsibly use their customers' personal information (*Not very dependent/ Not at all dependent*). A considerable proportion of respondents in these two industry groups, Retail/Manufacturing (11%) and Entertainment/Travel (10%), maintained there was little relationship between the success of their business and their ability to protect customers' privacy (*Neither dependent nor independent*) (see Figure 6).

**Figure 6: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information**

*"To what extent is the success of your business dependent upon your ability to protect and responsibly use your customers' personal information?"*



Beliefs about the relationship between business success and ability to protect customers' privacy do not seem to vary by the size of the organisation, but do, to some extent, differ according to whether the organisation has a privacy officer (see Table 26).

**Table 26: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by Size of Organisation and Location of Privacy Officer**

Response	Has Privacy Officer	No Privacy Officer
	(199) %	(361) %
Highly/somewhat dependent	88	76
Neither dependent /independent	5	8
Not very/ not at all dependent	7	15
Can't say	0	1
Total	100	100

*Base: All respondents.*

The majority (88%) of organisations with a designated privacy officer as well as the majority (76%) of organisations without a privacy officer said that the success of their business was dependent on protecting the privacy of customers' personal information

(*Highly dependent/ Somewhat dependent*). However, a substantial proportion of respondents (15%) in organisations without a privacy officer stated that the success of their business was *not* dependent on their ability to protect and responsibly use their customers' personal information (*Not very dependent/ Not at all dependent*).

Beliefs about the relationship between business success and ability to protect customers' privacy seem to vary by State location of the organisation (see Table 27).

**Table 27: Extent to Which Success of Business is Dependent on Protection and Responsible Use of Customers' Personal Information by State**

Response	VIC %	NSW %	QLD %	WA %
	(164)	(188)	(74)	(61)
Highly/somewhat dependent	84	80	80	74
Neither dependent /independent	7	6	9	5
Not very/ not at all dependent	9	13	8	21
Can't say	0	1	3	0
Total	100	100	100	100

*Base: All respondents in specified States.*

The majority of respondents in all States (74% to 84%) said that the success of their business was dependent on maintaining the privacy of their customers' personal information. However, a substantial proportion (21%) of respondents in Western Australia noted that the success of their business was not dependent on maintaining the privacy of customer information.

#### **4.5 Respondents' understanding of the term "Personal Information"**

Following questions about the importance of privacy of customers' personal information, the impact of a breach of privacy of such information on the organisation's public profile and customer relations, and the relationship between the success of the business and maintaining privacy of customers' personal information, respondents were asked to define the term "personal information".

The questions used to elicit respondents' definitions were: *What specific sorts of information does your organisation understand the term "personal information" to include?* Responses to these questions were coded into the categories shown in Table 28.

**Table 28: Respondents' Definitions of the Term "Personal Information"**

*"What specific sorts of information does your organisation understand the term "personal information" to include?"*

Response	Total (2261) %
Address (Private/Business)	18
Phone number (Private/Business)	16
Name	16
Income details	10
Age	7
Financial/ Taxation/ Credit card information/ Account details	6
Marriage status	5
Medical information	4
Business information/ ABNs/ Staff details/ Strategies	2
Living arrangements	2
Contractual information (eg pricing, trade agreements)/ Purchase history	2
Assets/ Liabilities/ Mortgage details/ Credit history	2
Employment history/ Resumes/ Occupation	2
Hobbies/ Interests	1
All information supplied by the client	1
E-mail addresses	1
Drivers' licence/ Driving record/ Car details	1
Personal information (unspecified)	1
Family/ Relatives/ Next of kin	<1
Passport details	<1
Client information/ Activities	<1
Criminal record	<1
Other	3
Can't say	<1
<b>TOTAL</b>	<b>100</b>

*Note:* Respondents could give more than one response.

Over 100 responses were in the following categories:

- *Address*
- *Phone number*
- *Name*
- *Income details*
- *Age*
- *Financial details*
- *Marriage status*

Between 31 and 100 responses were in the categories:

- *Medical information*
- *Business information*
- *Living arrangements*
- *Contractual information*
- *Assets/ Liabilities*
- *Employment history*
- *Hobbies/ Interests*

Between 10 and 30 responses were in the categories:

- *All information supplied by the client*
- *E-mail addresses*
- *Driving record*
- *Personal information (unspecified)*
- *Family/ Relatives*

#### **4.6 Organisational Factors and Customer Trust**

Responses to the question, *In your view, what is most likely to make customers trust your organisation with their personal information?* are shown in Table 29.

**Table 29: Reasons for Customers to Trust Organisation with Personal Information**

*“In your view, what is most likely to make customers trust your organisation with their personal information?”*

Response	Total (682) %
A good track record/ Proof that we do keep information confidential	28
Our reputation/ Good name/ Length of time we've been in business	23
Informing customers of our commitment to privacy/ Our procedures	16
We would not sell or give away private details/ We are professional/ Trustworthy	6
By building a close relationship with clients/ We work to build customer faith	4
They expect privacy from us/ Trust us	3
They have no choice/ They must give it to us or we cannot deal with them	2
A signed privacy or confidentiality agreement	2
The quality of our staff/ Good customer service	2
We are legally bound to confidentiality	1
Other	7
Can't say	6
TOTAL	100

*Note:* Respondents could give more than one reason.

The most frequently cited reasons (range 16% to 28% of responses) for customers trusting the organisation were:

- *A good track record/ Proof that we do keep information confidential*
- *Our reputation/ Good name/ Length of time we've been in business*
- *Informing customers of our commitment to privacy/ Our procedures*

Less common reasons (range 1% to 6%) given for customers trusting the organisation with personal information were in the categories:

- *We would not sell or give away private details/ We are professional/ Trustworthy*
- *By building a close relationship with clients/ We work to build customer faith*
- *They expect privacy from us/ Trust us*
- *They have no choice/ They must give it to us or we cannot deal with them*
- *A signed privacy or confidentiality agreement*
- *The quality of our staff/ Good customer service*
- *We are legally bound to confidentiality*

#### 4.7 Customer Service Factors in Dealing with Organisations

Respondents were asked to indicate what organisational factors were important in customers choosing to deal with the organisation: *Which of the following do you believe are most important to your customers when choosing whether or not to deal with your company?* Responses to this question are shown in Table 30.

**Table 30: Factors Believed to be Important to Customers in Choosing to Deal with Organisation**

*“Which of the following do you believe are most important to your customers when choosing whether or not to deal with your company?”*

Service Factor	First Mention	Second Mention	Third Mention	Fourth Mention	Fifth Mention
	%	%	%	%	%
Quality of product or service	53	24	13	7	2
Efficiency of service	16	30	30	17	6
Price	15	25	22	20	17
Protection or security of personal information	10	10	19	26	35
Convenience	3	11	15	30	40
Can't say	2	0	0	0	0
TOTAL	100	100	100	100	100

*Base: All respondents.*

The most frequently mentioned customer service factors across different sets of responses, in order of most important to least important were:

- *Quality of product or service*
- *Efficiency of service*
- *Price*
- *Convenience*
- *Protection or security of personal information*

#### 4.8 Privacy Guidelines in Organisations

Respondents were asked, *As far as you are aware, has an industry association relevant to your organisation developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information?* Responses to this question are shown in Table 31 and Table 32.

**Table 31: Existence of a Relevant Industry Association for Customer Privacy Issues**

*“As far as you are aware, has an industry association relevant to your organisation developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information?”*

Response	Total (560) %
YES – Industry association has developed guidelines	39
NO – Industry association has not developed guidelines	51
Can't say	10
Total	100

*Base: All respondents.*

A considerable number of respondents (10%) could not answer the question (*Can't say*).

Of those respondents who could answer the question, half the sample (51%) noted that there was *no* industry association relevant to their organisation that had developed guidelines outlining privacy protocols for customers' personal information. However, a substantial proportion of the sample (39%) said there was a relevant industry association that had developed privacy guidelines.



**Table 32: Existence of a Relevant Industry Association for Customer Privacy Issues by Type of Industry**

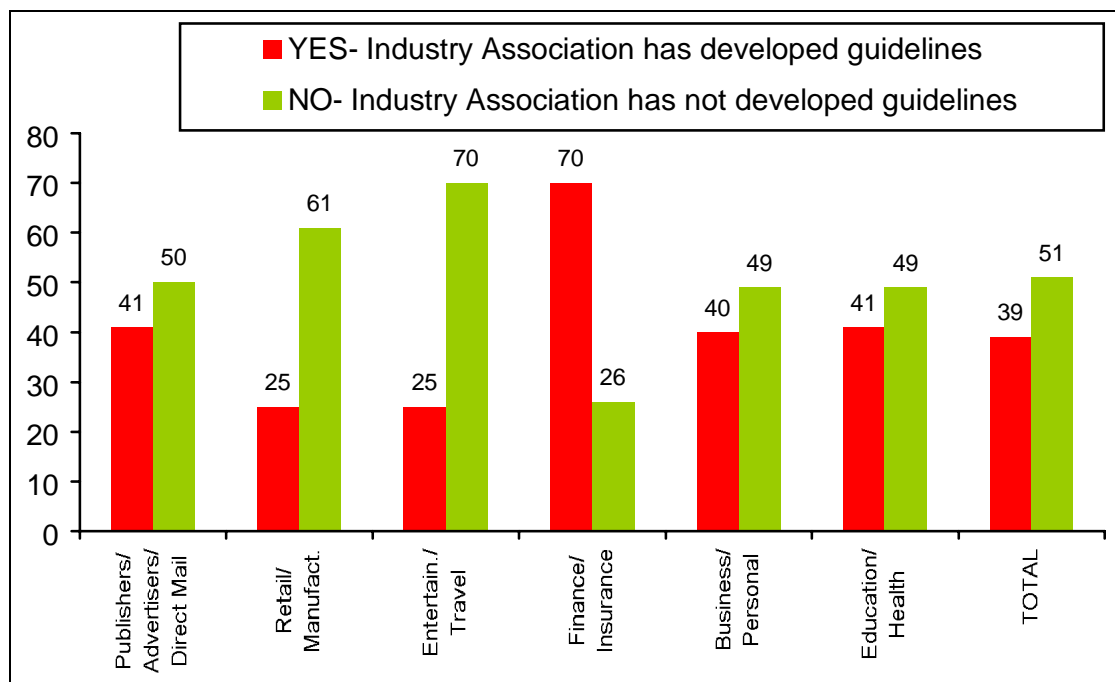
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
YES – Industry association has developed guidelines	41	25	25	70	40	41
NO – Industry association has not developed guidelines	50	61	70	26	49	49
Can't say	9	14	5	4	11	10
Total	100	100	100	100	100	100

*Base: All respondents.*

The pattern of responses to this question was consistent across all industry groups (except Finance/Insurance). That is, 49% to 70% of respondents in organisations within the different industry sectors said they did *not* have an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information. The exception to this pattern was the Finance/Insurance sector, where the majority (70%) of respondents said their organisations *did* have a relevant industry association that had developed privacy guidelines (see Figure 7).

**Figure 7: Existence of a Relevant Industry Association for Customer Privacy Issues**

*“As far as you are aware, has an industry association relevant to your organisation developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers’ personal information?”*



Responses to this question do seem to vary by the size of the organisation and on whether the organisation has a designated privacy officer (see Table 33).

**Table 33: Existence of a Relevant Industry Association for Customer Privacy Issues by Size of Organisation and Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
YES – Industry association has developed guidelines	35	45	48	35
NO – Industry association has not developed guidelines	55	47	45	55
Can't say	10	8	7	10
Total	100	100	100	100

*Base: All respondents.*

Most respondents (55%) in organisations with less than 20 employees said they *did not* have an industry association relevant to their organisation that had developed guidelines outlining privacy protocols for the collection, use and protection or storage of customers' personal information. For larger organisations, the distribution of responses to this question was evenly divided between those who *did* have industry association privacy guidelines (45%), and those who *did not* have such guidelines (47%).

The majority (55%) of respondents in organisations who did not have a privacy officer said they *did not* have an industry association that had developed privacy guidelines relevant to their organisation. In organisations that had a designated privacy officer, 48% of respondents said they *did* have an industry association that had developed relevant privacy guidelines, and 45% said they *did not* have industry association guidelines.

Responses to this question do seem to vary by State location of organisations (see Table 34).

**Table 34: Existence of a Relevant Industry Association for Customer Privacy Issues by State**

	VIC	NSW	QLD	WA
Response	(164) %	(188) %	(74) %	(61) %
YES – Industry association has developed guidelines	43	40	46	31
NO – Industry association has not developed guidelines	49	52	45	62
Can't say	8	8	9	7
Total	100	100	100	100

*Base: All respondents in specified States.*

In Victoria, New South Wales and Queensland, about half the respondents (45% to 52%) noted that there was no relevant industry association that had developed privacy guidelines for their organisations; between 40% and 46% of respondents in these States said there was a relevant industry association that had developed such guidelines. In Western Australia, the majority (62%) of respondents stated that their

organisations did not have a relevant industry association that had developed privacy guidelines for customer issues.

#### 4.9 Privacy Guidelines Followed by Organisations

Respondents were asked to indicate what type of privacy guidelines were currently followed by their organisations: *Does your organisation currently follow the privacy guidelines set out by the industry association, your own guidelines, some other guidelines, or no particular guidelines?*

Responses to this question are presented in Table 35. Note that this question was answered only by those who had access to industry association guidelines relevant to their organisations.

**Table 35: Type of Privacy Guidelines Followed by Organisations**

*“Does your organisation currently follow the privacy guidelines set out by the industry association, your own guidelines, some other guidelines, or no particular guidelines?”*

Response	Total (290) %
Guidelines set out by the industry association	60
Your own guidelines	35
Some other guidelines	2
No guidelines	2
Can't say	1
Total	100

*Note:* The figures in the table refer to a sub-sample of respondents: those who had access to industry association guidelines relevant to their organisations.

The majority (60%) of respondents said that their organisations followed the privacy guidelines set out by the relevant industry association. A substantial number of respondents (35%) said that they followed their own guidelines. Less than 5% of respondents stated that they followed some other guidelines or no particular guidelines.

The pattern of responses to the question about the type of privacy guidelines followed by organisations was consistent across industry groups (see Table 36).

**Table 36: Type of Privacy Guidelines Followed by Organisations by Type of Industry**

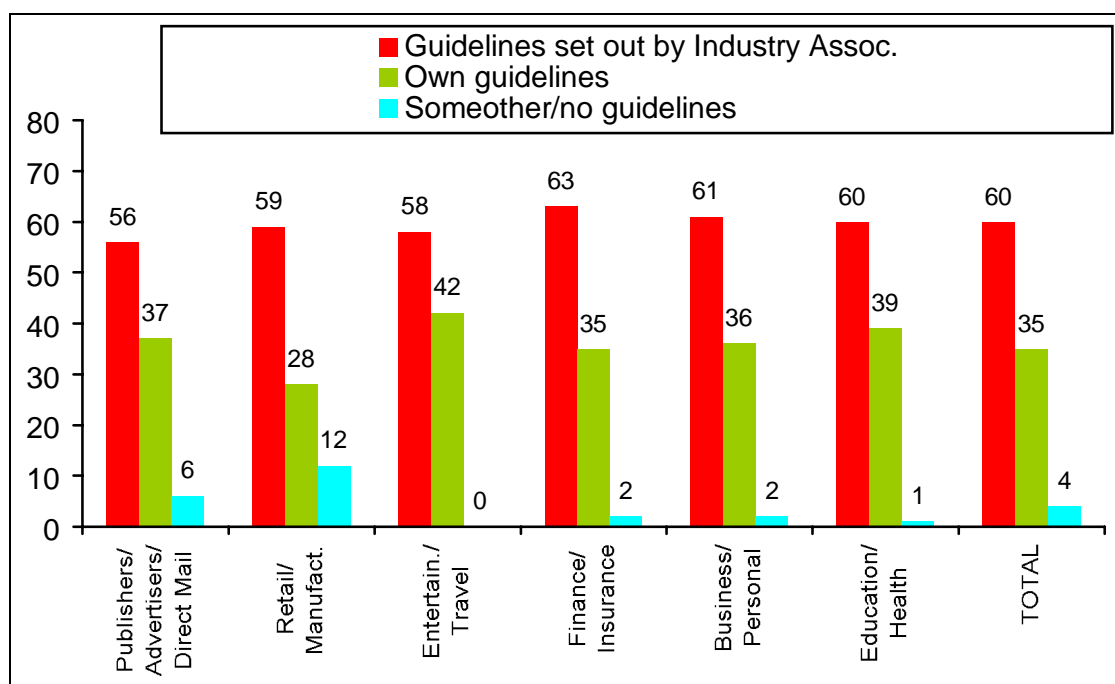
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(48) %	(41) %	(26) %	(75) %	(43) %	(57) %
Guidelines set out by the industry association	56	59	58	63	61	60
Your own guidelines	37	28	42	35	36	39
Some other guidelines	2	5	0	1	0	1
No guidelines	4	7	0	1	2	0
Can't say	1	1	0	0	1	0
Total	100	100	100	100	100	100

*Note:* The figures in the table refer to a subsample of respondents: those who had access to industry association guidelines relevant to their organisations.

Although the majority of respondents in each industry group (range 56% to 63%) said that they followed privacy guidelines set out by a relevant industry association, a substantial proportion of respondents in each industry group (range 28% to 42%) said their organisations followed their own privacy guidelines (see Figure 8).

**Figure 8: Type of Privacy Guidelines Followed by Organisations**

*“Does your organisation currently follow the privacy guidelines set out by the industry association, your own guidelines, some other guidelines, or no particular guidelines?”*



#### 4.10 Obtaining Information About Customers From Other Organisations

Respondents were asked: *Does your organisation obtain information about customers or potential customers from other organisations – for example, by purchasing, renting or swapping lists for marketing?* Responses to this question are shown in Table 37.

**Table 37: Organisation Obtaining Customer Information from Other Organisations**

Response	Total % (560)
Regularly	14
Occasionally	21
Never	64
Can't say	1
Total	100

*Base: All respondents.*

The majority of respondents (65%) said they *never* obtained information about customers from other organisations using these methods, 21% said they did so *occasionally*, and 14% said they *regularly* obtained customer information in these ways.

The pattern of responses to the question about obtaining customer information from other organisations was slightly different across industry groups (see Table 38).

**Table 38: Extent of Organisation Obtaining Customer Information from Other Organisations by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Regularly	17	10	7	22	17	11
Occasionally	33	26	18	9	13	20
Never	48	64	74	68	69	69
Can't say	2	0	1	1	1	0
Total	100	100	100	100	100	100

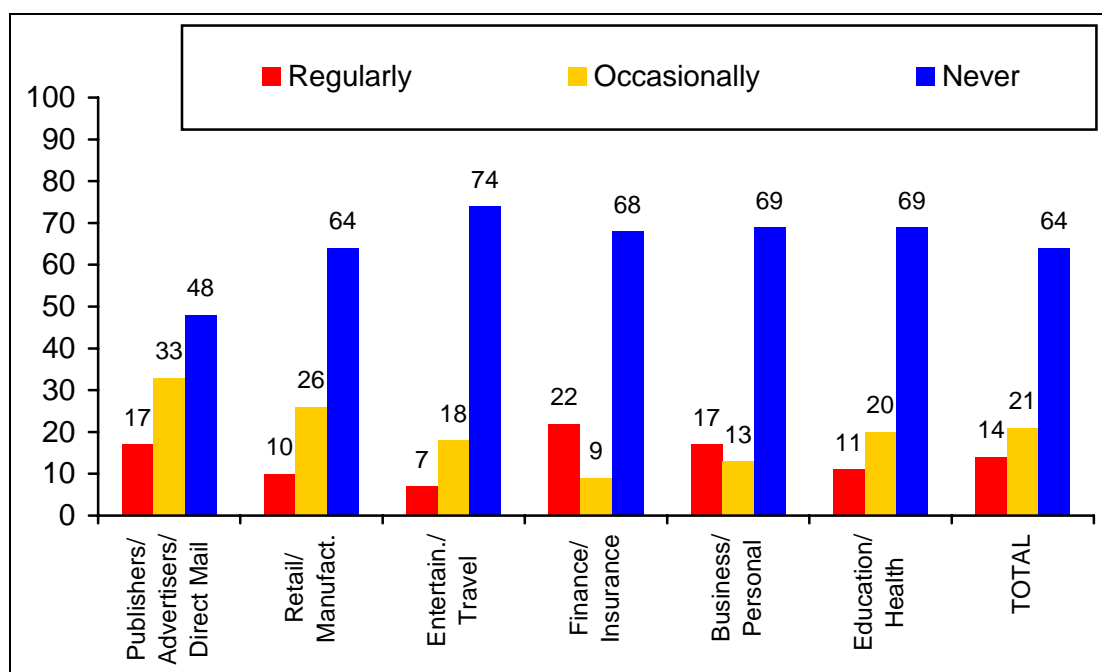
Base: All respondents.

The majority of respondents in all industry groups (range 64% to 74%, except Publishers/ Advertisers/ Direct Mail, 48%) said they *never* obtained information about customers or potential customers from other organisations.

A substantial proportion of respondents in all industry groups (range 13% to 33%, except Finance/Insurance, 9%) said they *occasionally* obtained customer information from other organisations. A considerable proportion of respondents in all industry groups (range 10% to 22%, except Entertainment/Travel, 7%) said they *regularly* obtained information about customers from other organisations. Of those organisations who *regularly* obtained customer information from other organisations, most were in the industry sectors Finance/Insurance, Business/Personal Services, and Publishers/Advertisers/Direct Mail (see Figure 9).

**Figure 9: Extent of Organisation Obtaining Customer Information from Other Organisations**

*“Does your organisation obtain information about customers or potential customers from other organisations – for example, by purchasing, renting or swapping lists for marketing?”*



#### 4.11 Providing Information About Customers To Other Organisations

Responses to the question, *Does your organisation sell, rent out or transfer customer details to other organisations regularly, occasionally or never?* are seen in Table 39.

**Table 39: Extent of Organisation Providing Customer Information to Other Organisations**

*“Does your organisation sell, rent out, or transfer customer details to other organisations regularly, occasionally, or never?”*

Response	Total % (560)
Regularly	4
Occasionally	5
Never	90
Can't say	1
Total	100

Base: All respondents.

A large majority of respondents (90%) said their organisations *never* sold, rented out or transferred customer details to other organisations, 5% said they did so *occasionally*, and 4% said they *regularly* provided customer information to other organisations in these ways.



The pattern of responses to the question about providing customer details to other organisations varied somewhat across industry groups (see Table 40).

**Table 40: Extent of Organisation Providing Customer Information to Other Organisations by Type of Industry**

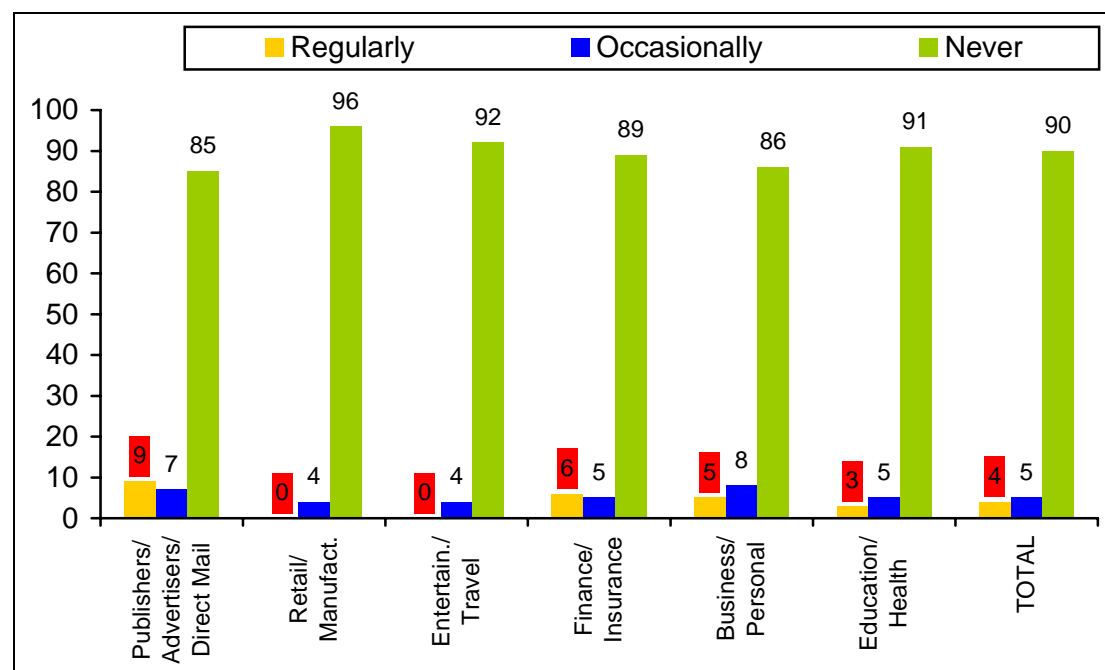
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Regularly	9	0	0	6	5	3
Occasionally	7	4	4	5	8	5
Never	85	96	92	89	86	91
Can't say	0	1	4	0	1	1
Total	100	100	100	100	100	100

Base: All respondents.

The majority of respondents in each industry group (range 85% to 96%) said they *never* provided information about customers to other organisations. Over 10% of respondents in three industry groups said they *regularly* or *occasionally* provided customer information to other organisations: Publishers/Advertisers/Direct Mail, Business/Personal Services, and Finance/Insurance (see Figure 10).

**Figure 10: Extent of Organisation Providing Customer Information to Other Organisations**

“Does your organisation sell, rent out, or transfer customer details to other organisations regularly, occasionally, or never?”



#### 4.12 Transfer of Customer Information Within Organisations

Respondents were asked: *Does your organisation regularly, occasionally or never transfer customer details internally for use in relation to different services or products offered by other sections of the company?* Responses to this question are shown in Table 41.

**Table 41: Extent of Organisation Transferring Customer Information Internally for Use in Other Sections of the Organisation**

*“Does your organisation regularly, occasionally, or never transfer customer details internally for use in relation to different services or products offered by other sections of the company?”*

Response	Total (560) %
Regularly	22
Occasionally	26
Never	48
Can't say	4
Total	100

*Base: All respondents.*

The distribution of responses to this question shows an even division between those organisations that *did* (48%) transfer customer details internally and those that *did not* (48%) transfer customer information within their organisations. Of those who did transfer customer information internally, 22% did this *regularly*, and 26% did this *occasionally*.

The pattern of responses to the question about internal transfer of customer information within organisations was somewhat different across industry groups (see Table 42).

**Table 42: Extent of Organisation Transferring Customer Information Internally for Use in Other Sections of the Organisation by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
----------	--	---------------------	----------------------	-----------------------	-----------------------------------	----------------------

	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Regularly	17	24	18	24	15	32
Occasionally	30	19	33	26	33	23
Never	50	54	47	48	45	41
Can't say	3	3	2	2	7	4
Total	100	100	100	100	100	100

*Base: All respondents.*

About half the organisations in all industry groups (range 41% to 54%) said they *never* transferred customer details internally for use in relation to different services or products offered by other sections of the company.

A substantial proportion of respondents in all industry groups said they *occasionally* (range 19% to 33%) or *regularly* (range 15% to 32%) transferred customer information within their organisations. Of those organisations who *regularly* transferred customer details internally, most were in three industry sectors: Education/Health, Retail/Manufacturing, and Finance/Insurance.

#### **4.13 Concerns About Transfer of Customers' Personal Information**

Respondents were presented a scenario about the transfer of customer personal information, without the customer's knowledge, from the respondent's organisation to another business. They were then asked to comment on the degree of concern this event might raise in their organisation.

*To what extent do you think the following practice would be of concern to customers? A customer provides his or her personal information such as name, address, date of birth, and interests to your organisation. Your organisation transfers this personal information to another business without the customer's knowledge. If your organisation were to do this, do you think this would be ...*

Responses to this question are shown in Table 43.

**Table 43: Degree of Concern About Transfer of a Customer's Personal Information to Another Business Without the Customer's Knowledge**

Response	Total (560) %
Of great concern	72
Of some concern	17
Neither of great nor little concern	3
Of little concern only	3
Of no concern at all	1
Can't say	4
Total	100

Base: All respondents.

A large majority of respondents (89%) said they considered the transfer of a customer's personal information to another business without the customer's knowledge would be of concern to their organisation (*Of great concern/ Of some concern*); only 4% said such an action would *not* be of much concern to their organisation (*Of little concern only/ Of no concern at all*).

Responses to the scenario about the transfer of a customer's personal information to another business without the customer's knowledge by industry group are shown in Table 44.

**Table 44: Concern About Transfer of Customer Information to Another Business Without the Customer's Knowledge, by Type of Industry**

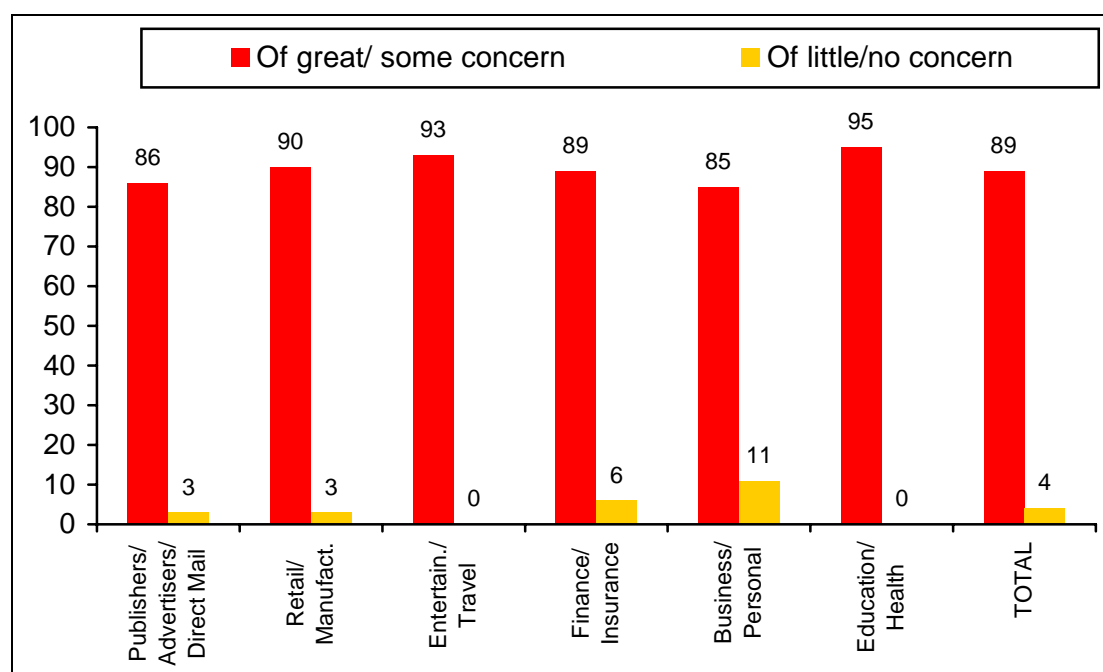
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Of great/some concern	86	90	93	89	85	95
Neither of great nor little	5	3	3	1	2	3

concern						
Of little/no concern	3	3	0	6	11	0
Can't say	6	4	4	4	2	2
Total	100	100	100	100	100	100

Base: All respondents.

The pattern of responses to the scenario was consistent across industry groups. The large majority of respondents in each industry group (range 85% to 95%) said the transfer of customer personal information in this manner would be of concern to their organisation (*Of great concern/ Of some concern*). Over 10% of responses in only one industry sector, Business/Personal Services, said the transfer of customer information in this manner would not be of much concern (see Figure 11).

**Figure 11: Degree of Concern About Transfer of a Customer's Personal Information to Another Business Without the Customer's Knowledge**



#### 4.14 Attitudes Toward Use and Protection of Customer Information

Respondents were asked to indicate their extent of agreement/disagreement with three statements about the way organisations use customer information and legal protection of such personal information. The statements and the distribution of responses to the statements are shown in Table 45, Table 46, and Table 47.

**Table 45: Attitudes Toward Use and Protection of Customer Personal Information (Statement 1)**

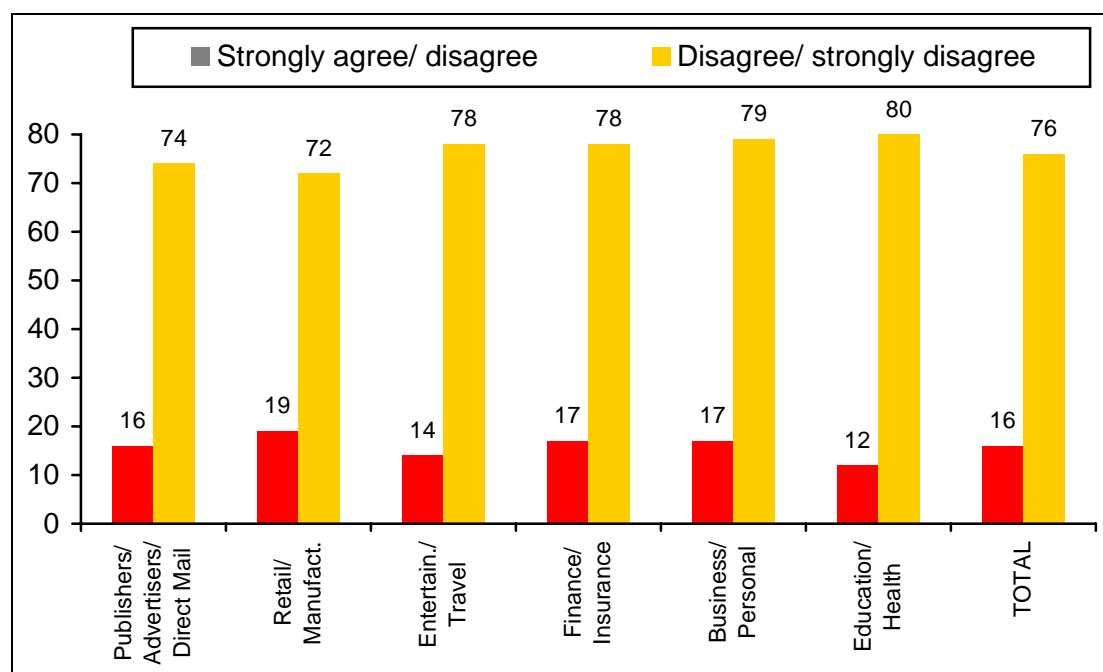
*“Businesses should be able to use the customer information they collect whenever, and for whatever purpose they choose.” Would you agree or disagree with this statement?*

Response	Total % (560)
Strongly agree	3
Agree	13
Neither agree nor disagree	6
Disagree	34
Strongly disagree	42

The majority of respondents (76%) disagreed (*Strongly disagree/ Disagree*) with the statement that businesses should be free to be able to use their customer information. However, a substantial portion of the sample (16%) agreed (*Strongly agree/ Agree*) with the statement. Of those who agreed with the statement, there was a relatively even spread across industry sectors (see Figure 12).

**Figure 12: Attitudes Toward Use and Protection of Customer Personal Information (Statement 1)**

*“Businesses should be able to use the customer information they collect whenever, and for whatever purpose they choose.”*



**Table 46: Attitudes Toward Use and Protection of Customer Personal Information (Statement 2)**

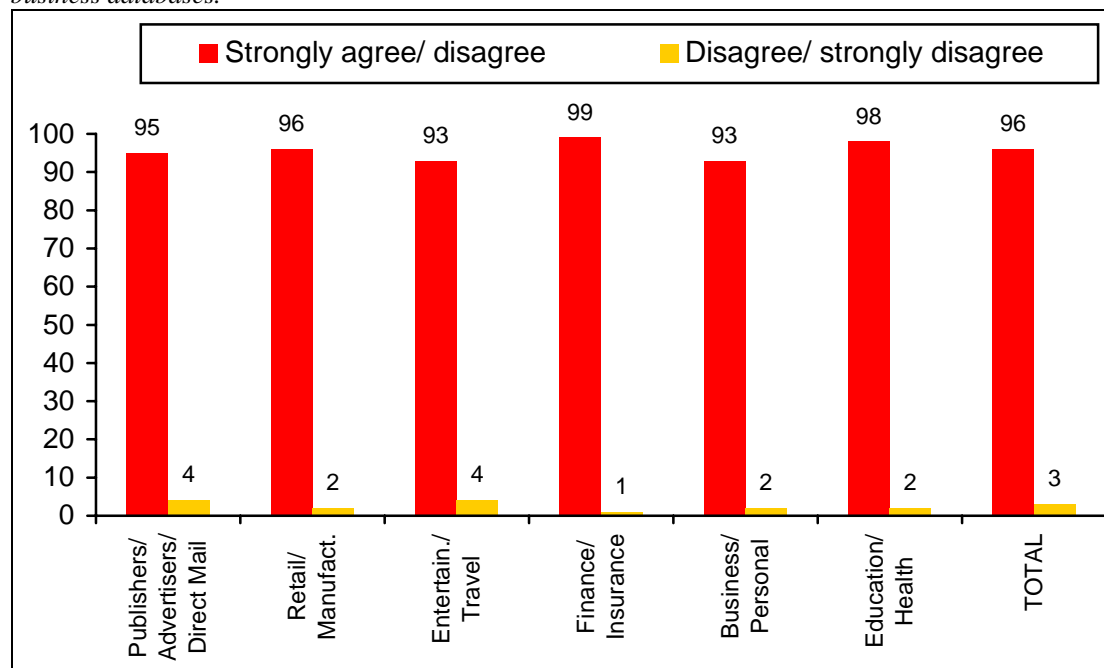
*“It is reasonable that there should be laws to protect consumers’ personal information held on business databases.” Would you agree or disagree with this statement?*

Response	Total % (560)
Strongly agree	55
Agree	40
Neither agree nor disagree	1
Disagree	2
Strongly disagree	1

Most respondents (96%) agreed (*Strongly agree/ Agree*) with the statement that there should be legal protection for consumers’ personal information held on databases. Only 3% of the sample disagreed (*Strongly disagree/ Disagree*) with the statement. Respondents who disagreed with the statement were evenly distributed among the different industry sectors (see Figure 13).

**Figure 13: Attitudes Toward Use and Protection of Customer Personal Information (Statement 2)**

*“It is reasonable that there should be laws to protect consumers’ personal information held on business databases.”*



**Table 47: Attitudes Toward Use and Protection of Customer Personal Information (Statement 3)**

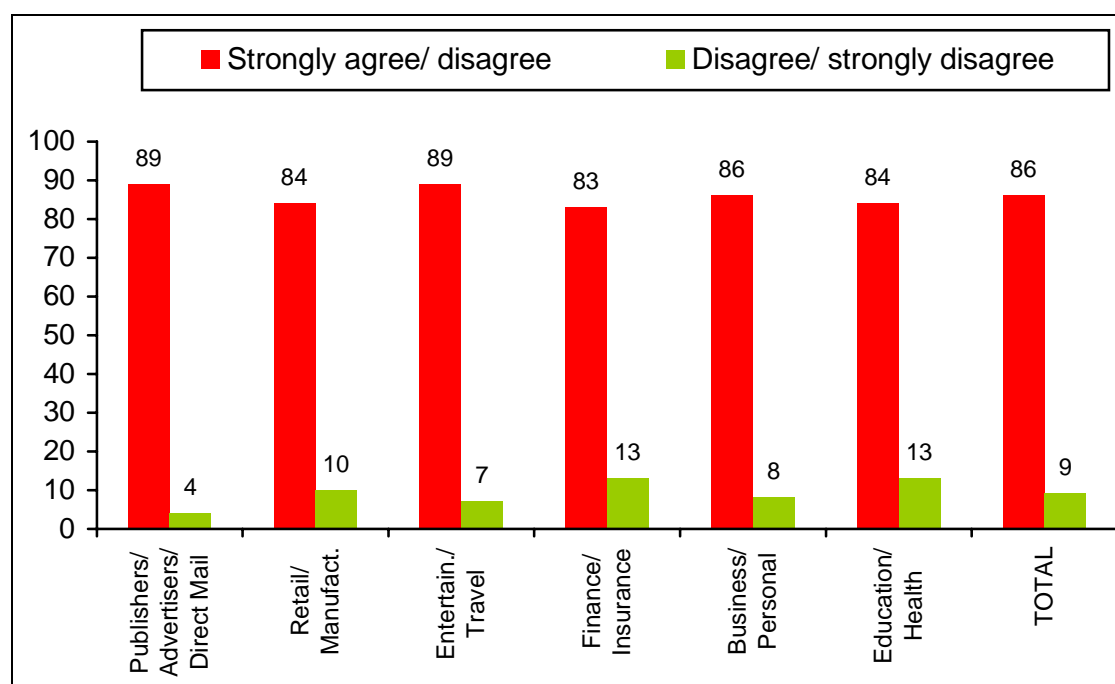
*“An organisation’s customer database is a valuable commercial asset.” Would you agree or disagree with this statement?*

Response	Total % (560)
Strongly agree	48
Agree	38
Neither agree nor disagree	3
Disagree	8
Strongly disagree	2

A large majority of respondents (86%) agreed (*Strongly agree/ Agree*) with the statement that an organisation’s customer database is a valuable commercial asset. Less than 10% of the sample (9%) disagreed (*Strongly disagree/ Disagree*) with this statement. Of those who disagreed with the statement, there was a relatively even spread across industry sectors (see Figure 14).

**Figure 14: Attitudes Toward Use and Protection of Customer Personal Information (Statement 3)**

*“An organisation’s customer database is a valuable commercial asset.”*





#### 4.15 Awareness and Knowledge of Federal Privacy Laws

Respondents were asked several questions about their awareness and knowledge of Federal privacy laws. The questions and the distribution of responses to the questions are shown in Table 48, Table 49, and Table 50.

**Table 48: Awareness and Knowledge of Federal Privacy Laws (Question 1)**

*“Were you aware of the existence of federal privacy laws before this interview?”*

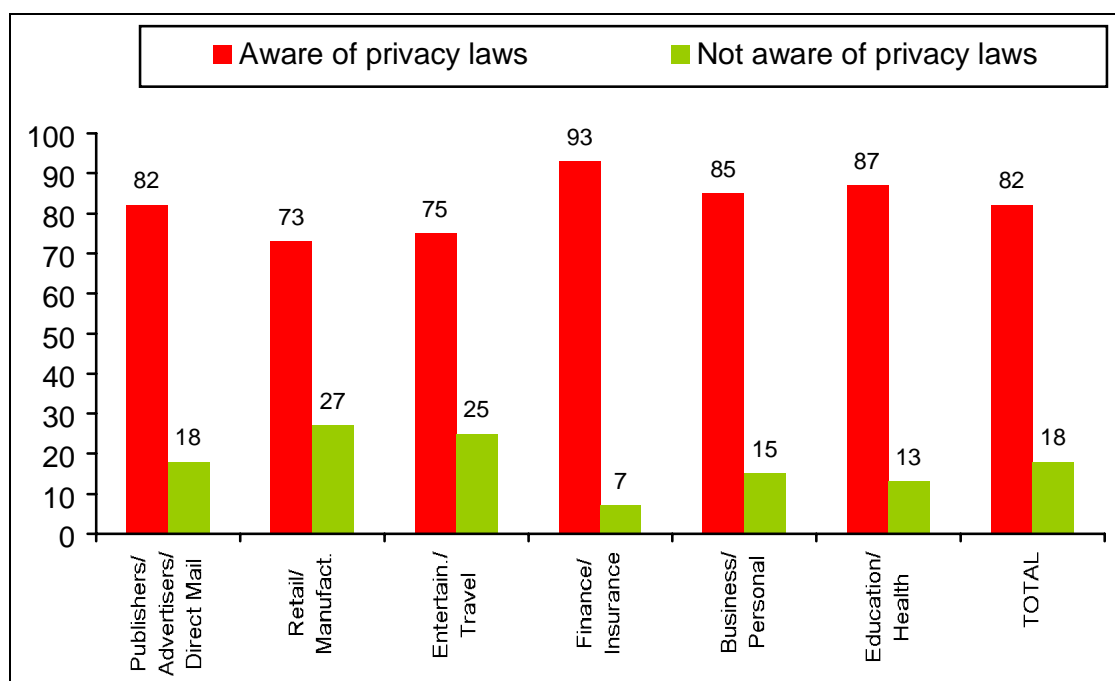
Response	Total (560) %
YES	82
NO	18

The majority of the sample (82%), and the majority of respondents in each industry sector (range 73% to 93%) said that, before the interview, they *were aware of the existence of Federal privacy laws*.

However, a substantial portion of the sample (18%) said they *were not aware* of the existence of Federal privacy laws before the interview. Of those respondents who were not aware of the Federal privacy laws, most were in the industry sectors Retail/Manufacturing and Entertainment/Travel (see Figure 15).

**Figure 15: Awareness and Knowledge of Federal Privacy Laws (Question 1)**

*“Were you aware of the existence of federal privacy laws before this interview?”*



**Table 49: Awareness and Knowledge of Federal Privacy Laws (Question 2)**

“Were you aware of what organisations the federal privacy laws applied to, before this interview?”

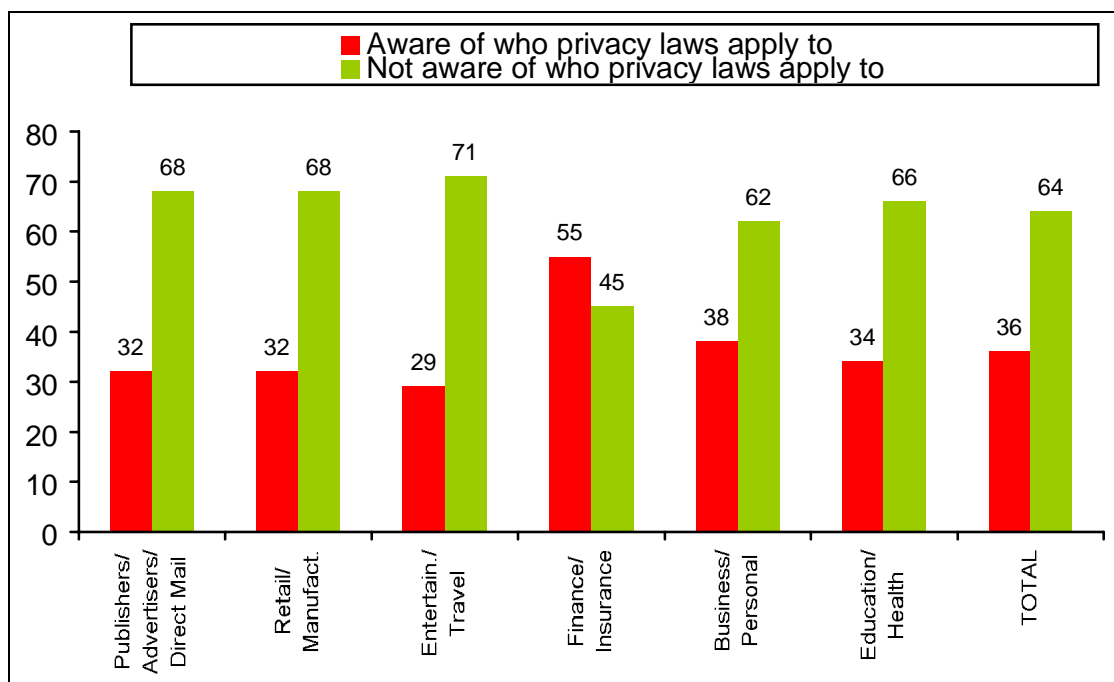
Response	Total % (560)
YES	36
NO	64

Less than 40% of the sample (36%) said that, before the interview, they *were aware* of what organisations the Federal privacy laws applied to. This pattern of moderate awareness of organisational applicability of Federal privacy laws was consistent across all industry groups (range 29% to 38%) except Finance/Insurance, where the majority of respondents in this group (55%) were aware of the applicability of the privacy laws.

A considerable proportion of respondents (64%) said that, before the interview, they *were not aware* of what organisations the Federal privacy laws applied to. The majority of respondents in all industry groups (range 62% to 71%, except Finance/Insurance, 45%) said that they were *not aware* of the organisational applicability of Federal privacy laws (see Figure 16).

**Figure 16: Awareness of which organisations the Federal Privacy Laws applied to (Question 2)**

“Were you aware of what organisations the federal privacy laws applied to, before this interview?”



**Table 50: Awareness and Knowledge of Federal Privacy Laws (Question 3)**

“Before this interview, were you aware that new federal privacy laws come into effect in December this year?”

Response	Total (560) %
YES	37
NO	63

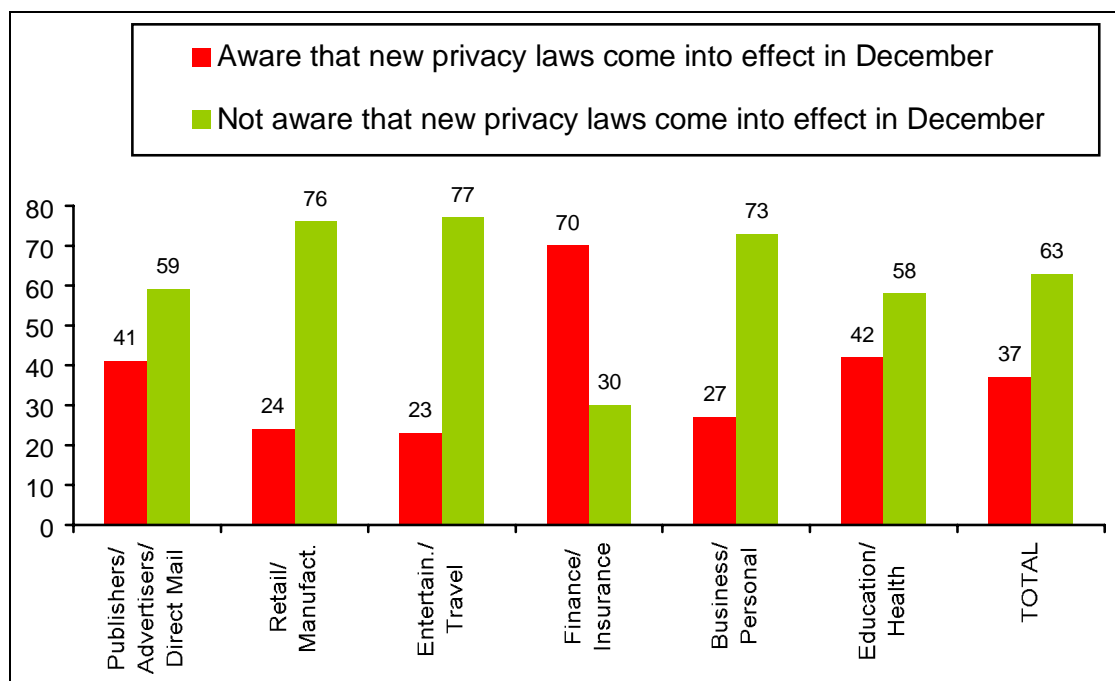
Less than 40% of the sample (37%) said that, before the interview, they *were aware* that new Federal privacy laws come into effect in December 2001. This pattern of moderate awareness of the privacy laws was consistent across all industry groups (range 23% to 41%) except Finance/Insurance, where the majority of respondents in this group (70%) were aware that the new privacy laws would come into effect later in the year.

A large portion of the sample (63%) said that, before the interview, they *were not aware* that new Federal privacy laws come into effect in December 2001. The majority of respondents in all industry groups (range 58% to 77%, except

Finance/Insurance, 30%) said that they were *not* aware of when the new Federal privacy laws would come into effect (see Figure 17).

**Figure 17: Awareness and Knowledge of Federal Privacy Laws (Question 3)**

*“Before this interview, were you aware that new federal privacy laws come into effect in December this year?”*



Responses to the questions about awareness of the Federal privacy laws by size of organisation and location of privacy officers are shown in Table 51, Table 52, and Table 53.

**Table 51: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 1)**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
YES	79	85	86	79
NO	21	15	14	21
Total	100	100	100	100

Base: All respondents.

**Table 52: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 2)**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
YES	31	43	45	32
NO	69	57	55	68
Total	100	100	100	100

Base: All respondents.

**Table 53: Awareness and Knowledge of Federal Privacy Laws by Size of Organisation and Location of Privacy Officer (Question 3)**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315) %	(245) %	(199) %	(361) %
YES	30	45	51	29
NO	70	55	49	71
Total	100	100	100	100

Base: All respondents.

Small organisations (i.e., those with less than 20 employees) showed somewhat less awareness of the Federal privacy laws than larger organisations. About 20% of respondents from small organisations, compared to 15% of those in larger organisations, were *not* aware of the existence of Federal privacy laws before the interview. Nearly 70% of respondents from small organisations, compared to 57% in larger organisations, were *not* aware of what organisations the Federal privacy laws applied to before the interview. About 70% of those in small organisations, compared to 55% in larger organisations, were *not* aware that new Federal privacy laws come into effect in December this year.

Respondents in organisations that did not have a designated privacy officer showed slightly less awareness of the Federal privacy laws than respondents from organisations without privacy officers. About 20% of those in organisations without privacy officers, compared to 14% of those in organisations with privacy officers, were *not* aware of the existence of Federal privacy laws before the interview. Nearly 70% of respondents from organisations without privacy officers, compared to 55% of those with privacy officers, were *not* aware of what organisations the Federal privacy laws applied to before the interview. About 70% of those in organisations without a privacy officer, compared to 49% of those in with privacy officers, were *not* aware that new Federal privacy laws come into effect in December 2001.

#### 4.16 Organisational Knowledge About New Federal Privacy Laws

Responses to the question, *At this stage, how would you describe your organisation's level of knowledge concerning the new privacy laws?* are shown in Table 54.

**Table 54: Extent of Organisational Knowledge About New Privacy Laws**

*“At this stage, how would you describe your organisation's level of knowledge concerning the new privacy laws?”*

Response	Total (560) %
A high level of knowledge	12
Some knowledge	32
Very little knowledge	34
No knowledge at all	18
Can't say	4
Total	100

*Base: All respondents.*

More than half the sample (52%) said their organisations had *very little knowledge* or *no knowledge at all* about the new privacy laws. Only 12% of respondents said their organisations had a *high level of knowledge* concerning the new privacy laws. A substantial proportion of respondents (32%) said their organisations had *some knowledge* about the new privacy laws.

There were some differences in responses to this question across industry groups (see Table 55).

**Table 55: Extent of Organisational Knowledge About New Privacy Laws by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
A high level of knowledge	15	7	3	29	11	11
Some knowledge	27	27	34	43	29	38
Very little knowledge	40	38	34	21	37	31
No knowledge at all	14	26	25	5	23	14
Can't say	4	2	4	2	0	6
Total	100	100	100	100	100	100

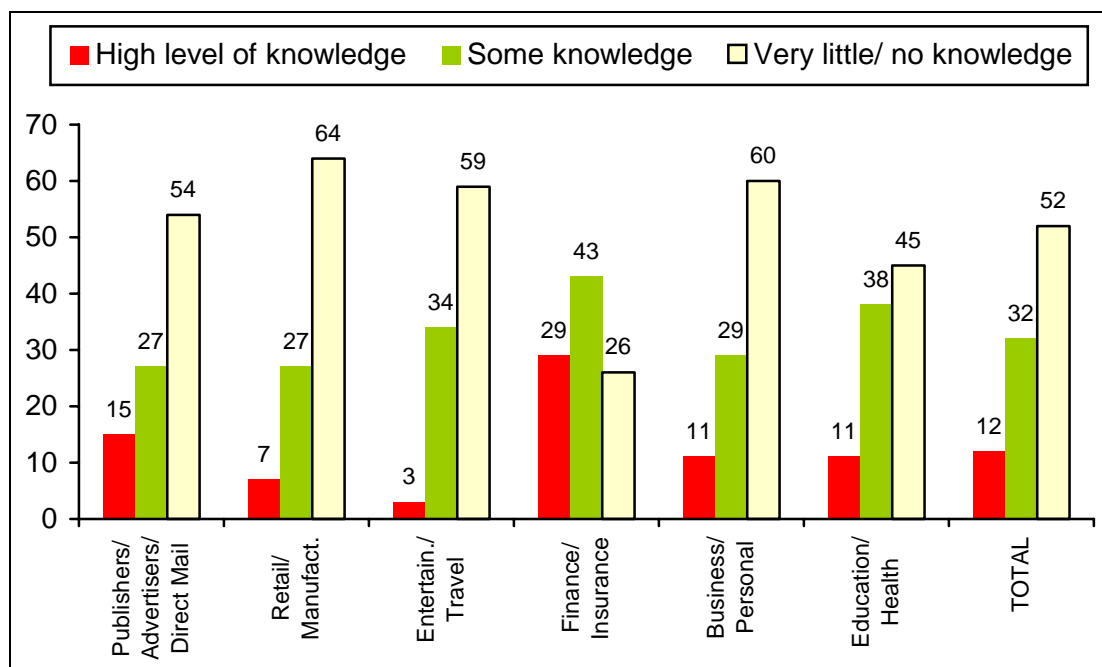
*Base: All respondents.*

Respondents in the Finance/Insurance sector seem to have greatest confidence in the level of knowledge held by their organisations about the new privacy laws. Nearly 30% of respondents in Finance/Insurance said their organisations had a *high level of knowledge*, 43% said their organisations had *some knowledge*, and 26% said their organisations had *very little knowledge* or *no knowledge at all* about the new privacy laws.

The majority of respondents in all other industry sectors (range 54% to 64%, except Education/Health, 45%) said their organisation had *very little knowledge* or *no knowledge at all* about the new privacy laws. Less than 20% of respondents in all industry sectors (range 3% to 15%, except Finance/Insurance, 29%) said their organisation had a *high level of knowledge* about the new privacy laws (see Figure 18).

**Figure 18: Extent of Organisational Knowledge About New Privacy Laws**

“At this stage, how would you describe your organisation’s level of knowledge concerning the new privacy laws?”



Organisational knowledge about the new privacy laws seems to vary by the size of the organisation and whether the organisation has a privacy officer (see Table 56).

**Table 56: Extent of Organisational Knowledge About New Privacy Laws by Size of Organisation and Location of Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees (315) %	≥ 20 Employees (245) %	Has Privacy Officer (199) %	No Privacy Officer (361) %
A high level of knowledge	10	16	22	7
Some knowledge	27	39	38	29
Very little knowledge	37	30	29	37
No knowledge at all	23	13	10	23
Can't say	3	2	1	4
Total	100	100	100	100

Base: All respondents



Most respondents (60%) in organisations with less than 20 employees said their organisation had *very little knowledge* or *no knowledge at all* about the new privacy laws; 43% of respondents in larger organisations gave similar responses. Only 10% of respondents in small organisations, compared to 16% of those in larger organisations, said their organisation had a *high level of knowledge* about the new privacy laws.

The majority of respondents (60%) in organisations without a privacy officer said their organisation had *very little knowledge* or *no knowledge at all* about the new privacy laws. In contrast, 39% of respondents in organisations with a designated privacy officer gave these responses. Only 7% of respondents in organisations without a privacy officer, compared to 22% in organisations with a privacy officer, said their organisation had a *high level of knowledge* about the new privacy laws.

#### 4.17 Impact of New Federal Privacy Laws on Businesses

Respondents were asked to indicate the extent to which the new Federal privacy laws impact on businesses: *As far as you are aware, to what extent do these laws currently impact upon the way your business is conducted?* The distribution of responses to this question is shown in Table 57.

**Table 57: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted**

*“As far as you are aware, to what extent do these laws currently impact upon the way your business is conducted?”*

Response	Total (560) %
To a large extent	18
To some extent	40
Not at all	39

A majority of respondents (58%) said they thought the new privacy laws do have an impact upon the way their business is currently conducted (*To a large extent/ To some extent*). However, a substantial proportion of respondents (39%) said the new privacy laws did *not* impact on the way their business is conducted (*Not at all*).

Responses to the question about the impact of the new laws on the conduct of business by industry group are shown in Table 58.

**Table 58: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted by Type of Industry**

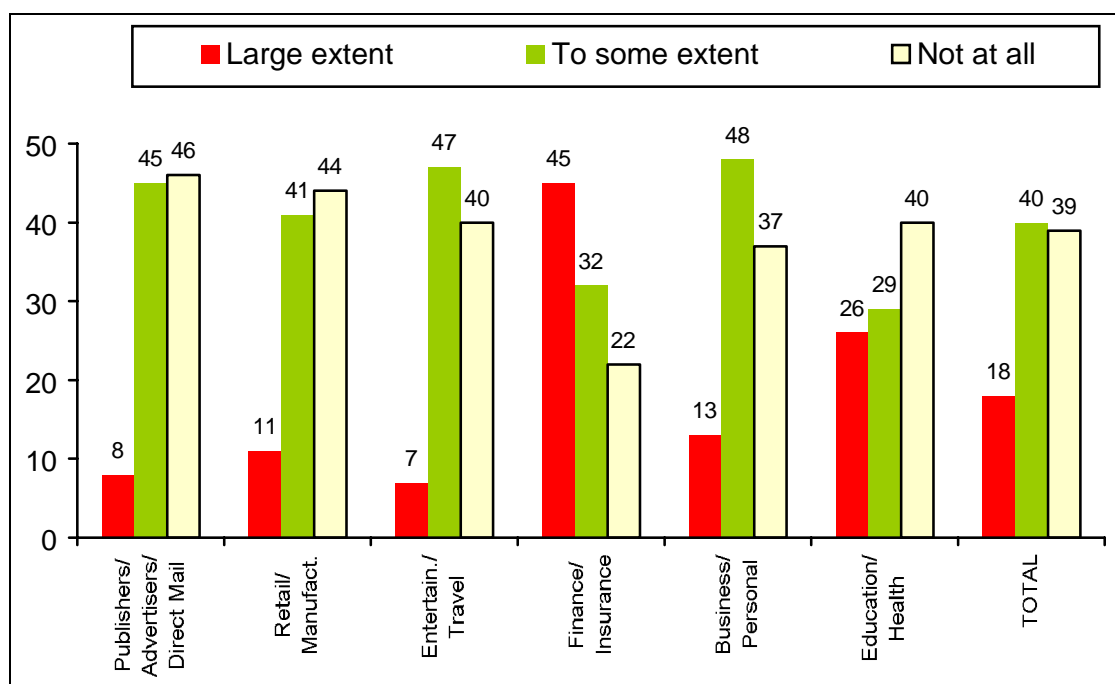
<b>Response</b>	<b>Publishers/ Advertisers/ Direct Mail</b>	<b>Retail/ Manufact</b>	<b>Entertain/ Travel</b>	<b>Finance/ Insurance</b>	<b>Business/ Personal Services</b>	<b>Education/ Health</b>
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
To a large extent	8	11	7	45	13	26
To some extent	45	41	47	32	48	29
Not at all	46	44	40	22	37	40

The majority of respondents in each industry group (range 52% to 77%) said the new laws do currently impact upon the way their business is conducted (*To a large extent/ To some extent*).

The industry sectors that seem to be most affected are Finance/Insurance and Business/Personal Services, where a large proportion of respondents (77% and 61% respectively) noted the new laws had *to a large extent* or *to some extent* had an impact on the way their business is conducted (see Figure 19).

**Figure 19: Extent of Impact of New Federal Privacy Laws**

*“As far as you are aware, to what extent do these laws currently impact upon the way your business is conducted?”*



Responses to this question by the size of organisation are shown in Table 59.

**Table 59: Extent of Impact of New Federal Privacy Laws on the Way Business is Conducted by Size of Organisation**

Response	<20 Employees (315) %	≥ 20 Employees (245) %
To a large extent	15	21
To some extent	37	43
Not at all	44	33
Can't say	4	3
Total	100	100

Base: All respondents

Large organisations seem to be affected by the new laws more than small organisations. A somewhat higher percentage of respondents in larger organisations (64%), compared to small organisations (52%) said the new laws did currently impact upon the way their business is conducted (*To a large extent/ To some extent*).

#### 4.18 Attitudes to Changes to the Federal Privacy Legislation

Responses to the question, *Would you view the changes to the Federal privacy legislation as a positive or negative event for the business community?* are shown in Table 60. Note that only those respondents who stated that their organisation had a high level or some knowledge concerning the new Federal privacy laws were asked to respond to this question.

**Table 60: Impact of Changes to the Federal Privacy Legislation for the Business Community**

*“Would you view the changes to the federal privacy legislation as a positive or negative event for the business community?”*

Response	Total (250) %
Very positive	29
Somewhat positive	44
Neither positive nor negative	10
Somewhat negative	12
Very negative	0
Can't say	5
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisation had a high level or some knowledge concerning the new federal privacy laws.

Most respondents (73%) said they viewed the changes to the Federal privacy legislation as a positive event (*Very positive/ Somewhat positive*); only 12% viewed the changes as a negative event for the business community (*Somewhat negative/ Very negative*).

#### **4.19 Reasons for Viewing Changes to Federal Privacy Legislation as Positive**

Respondents who said that they viewed changes to the Federal privacy legislation as a positive event for the business community were asked to give reasons for their statements; their responses are shown in Table 61.

**Table 61: Reasons for Viewing Changes to Federal Privacy Legislation as Positive for the Business Community**

*“Could you please tell me your main reasons for saying the changes are a positive event for the business community?”*

Main Reason	Total (178) %
It will be beneficial to our business/ Improves relations/ Builds business	16
Gives consumers more confidence about the way personal details are kept	14
Everyone has a right to know which details are kept about them	13
Lessens misuse of private information/ Prevent unauthorised intrusion	12
Protects confidentiality/ Consumer protection/ Safety	11
Will make businesses more honest/ Ethical	11
Trust/ Builds trust	5
There is currently too much passing around of information	4
Regulation puts everyone on the same level	4
Provides us with correct information	3
Regulation is necessary as so much personal information is available	2
Laws should be very strict/ High standards	2
We value our clients and would not misuse their information	2
Brings Australia more in line with Europe	1
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who viewed the changes to the federal privacy legislation as positive for the business community.

The most common reasons (representing over 10% of responses in each category) given for viewing changes to the Federal privacy legislation as *positive* for the business community were:

- *It will be beneficial to our business/ Improves relations/ Builds business*
- *Gives consumers more confidence about the way personal details are kept*
- *Everyone has a right to know which details are kept about them*
- *Lessens misuse of private information/ Prevent unauthorised intrusion*
- *Protects confidentiality/ Consumer protection/ Safety*
- *Will make businesses more honest/ Ethical*

Less commonly cited reasons (representing less than 10% of responses in each category) for the viewing the changes as a *positive* event were:

- *Trust/ Builds trust*
- *There is currently too much passing around of information*
- *Regulation puts everyone on the same level*
- *Provides us with correct information*
- *Regulation is necessary as so much personal information is available*
- *Laws should be very strict/ High standards*
- *We value our clients and would not misuse their information*
- *Brings Australia more in line with Europe*

#### **4.20 Reasons for Viewing Changes to Federal Privacy Legislation as Negative**

Respondents who said that they viewed changes to the Federal privacy legislation as a negative event for the business community were asked to give reasons for their statements; their responses are shown in Table 62.

**Table 62: Main Reasons for Viewing New Privacy Legislation as Negative**

Main Reason	Total % (30)
Expensive to implement	33
Too restrictive for us/ Less flexibility	23
Need more resources to implement	20
Extra work/ Red tape	10
Too much to do following GST	7
It may hurt other (less regulated) businesses	7
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who viewed the changes to the Federal privacy legislation as negative for the business community.

The most common reasons (representing over 10% of responses in each category) given for viewing changes to the Federal privacy legislation as *negative* for the business community were:

- *Expensive to implement*
- *Too restrictive for us/ Less flexibility*
- *Need more resources to implement*

Less commonly cited reasons (representing less than 10% of responses in each category) for the viewing the changes as a *negative* event were:

- *Extra work/ Red tape*
- *Too much to do following GST*
- *It may hurt other (less regulated) businesses*

#### 4.21 Impact of New Federal Privacy Laws on Consumers

Responses to the question, *Would you view the changes to the Federal privacy legislation as a positive or negative event for consumers?* are shown in Table 63. Note that only those respondents who stated that their organisation had a high level or some knowledge concerning the new Federal privacy laws were asked to respond to this question.

**Table 63: Impact of Changes to the Federal Privacy Legislation for Consumers**

*“Would you view the changes to the federal privacy legislation as a positive or negative event for consumers?”*

Response	Total (250) %
Very positive	54
Somewhat positive	32
Neither positive nor negative	5
Somewhat negative	5
Very negative	0

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisation had a high level or some knowledge concerning the new Federal privacy laws.

Most respondents (86%) said they viewed the changes to the Federal privacy legislation as a positive event for consumers (*Very positive/ Somewhat positive*); only

5% viewed the changes as a negative event for the business community (*Somewhat negative/ Very negative*).

#### 4.22 Internet Privacy Issues Relating to Clients' Personal Information

Respondents were asked several questions about privacy issues affecting client personal information on the Internet.

Responses to the question, *In your view, when dealing over the Internet, do customers have more concerns about the security of their personal details than usual, fewer concerns or about the same?* are shown in Table 64.

**Table 64: Extent of Customer Concerns About Security of Personal Information on the Internet**

*"In your view, when dealing over the Internet, do customers have more concerns about the security of their personal details than usual, fewer concerns, or about the same?"*

Response	Total (560) %
More concerns	64
Fewer concerns	6
About the same	22
Can't say	8
Total	100

*Base: All respondents.*

A majority of the sample (64%) said they thought customers would have *more concerns* about the security of their personal details than usual when dealing over the Internet; only 6% said they thought customers would have *fewer concerns* than usual. However, a substantial proportion of the sample (22%) noted that customer concerns about the security of personal information on the Internet would be *about the same* as usual.

Responses to the question about privacy of clients' personal information on the Internet by industry group showed similar patterns (see Table 65).



**Table 65: Extent of Customer Concerns About Security of Personal Information on the Internet by Type of Industry**

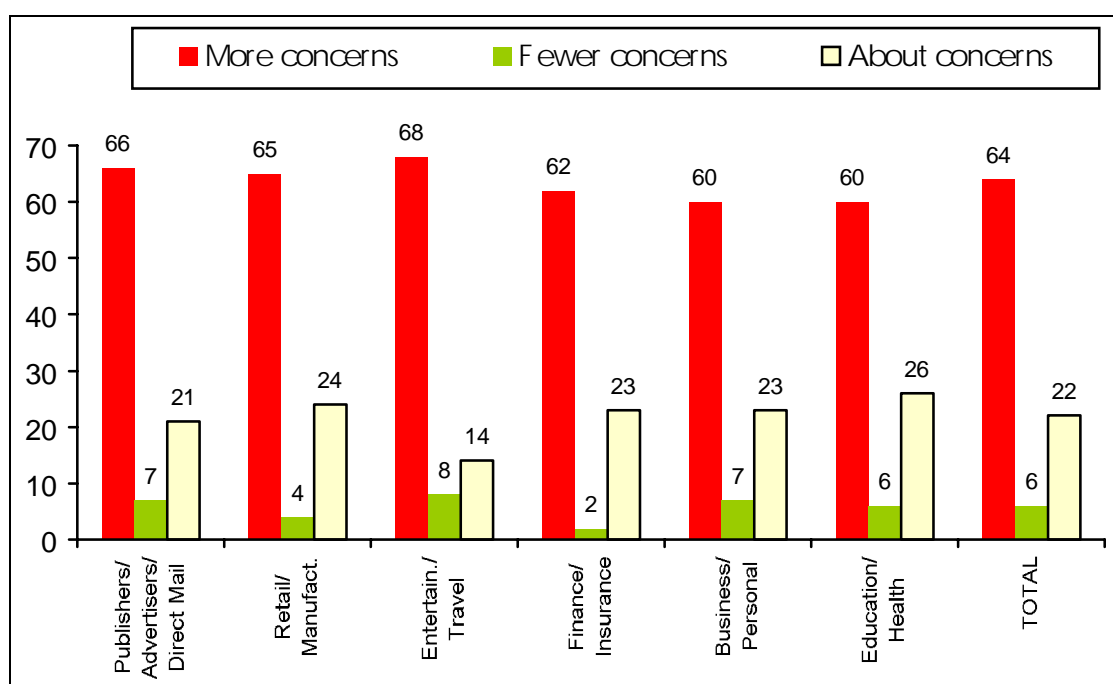
<b>Response</b>	<b>Publishers/ Advertisers/ Direct Mail</b>	<b>Retail/ Manufact</b>	<b>Entertain/ Travel</b>	<b>Finance/ Insurance</b>	<b>Business/ Personal Services</b>	<b>Education/ Health</b>
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
More concerns	66	65	68	62	60	60
Fewer concerns	7	4	8	2	7	6
About the same	21	24	14	23	23	26
Can't say	6	7	10	13	10	8

*Base: All respondents.*

The majority of respondents in each industry group (range 60% to 68%) said they believed that when dealing over the Internet, customers have *more concerns* about the security of their personal information.

The industry sector that seems most concerned about customers' views about the security of personal information on the Internet is Entertainment/Travel, where a large proportion of respondents (68%) said customers would have *more concerns* about the security of their information when dealing over the Internet; only 14% of this group said customers' concerns about privacy of their information on the Internet would be *about the same* as usual (see Figure 20).

**Figure 20: Extent of Customer Concerns About Security of Personal Information on the Internet**



#### 4.23 Organisation Websites

Respondents were asked: *Has your organisation established, or does it intend to establish, a website?* Responses to this question are shown in Table 66.

**Table 66: Existence of Organisation Website**

*“Has your organisation established, or does it intend to establish, a website?”*

Response	Total (560) %
Already established	79
Intend to establish	10
Maybe	3
No – No site or intention	8

A large majority of the sample (79%) said they had *already established* a website, and another 13% said their organisation *intended* to establish a website. Only 8% said their organisation had *not established* a website or had *no intention* of establishing one.

The pattern of responses to the question about organisation websites was similar across industry groups (see Table 67).

**Table 67: Existence of Organisation Website by Type of Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Already established	79	81	81	77	67	84
Intend to establish	15	7	8	13	10	9
Maybe	2	5	4	0	3	1
No – No site or intention	3	7	7	10	20	5

The majority of respondents (range 67% to 84%) in all industry groups said they had *already established* a website. The proportion of respondents in industry groups who said their organisation intended to establish a website ranged from 10% (Education/Health) to 17% (Publishers/Advertisers/Direct Mail). The industry groups least likely to establish a website (*No website or intention*) were: Business/Personal Services (20%) and Finance/Insurance (10%).

#### 4.24 Protecting Client Privacy On-line

Respondents were asked, *What special measures, if any, would you need to consider in order to protect client privacy on-line?* Responses to this question are shown in Table 68. Note that only those respondents who stated that their organisation had already established a website, or intended to establish a website were asked to respond to this question.

**Table 68: Special Measures Needed to Protect Client Privacy On-line**

*“What special measures, if any, would you need to consider in order to protect client privacy on-line?”*

Response	Total (417) %
Security protocols	23
Security of data (Fire walls, etc.)	16
On-line privacy policy	13
We do not have client details on-line	10
It’s already secure/ Have systems in place/ We’ll ensure security (unspecified)	6
Issue passwords/ Password protection/ Codes for access	2
Other	4
Can’t say	26
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisation had already established a website or intended to establish a website.

The most common responses (representing over 10% of responses in each category) given for this question were:

- *Security protocols*
- *Security of data (Fire walls, etc.)*
- *On-line privacy policy*

Less common responses (representing less than 10% of responses in each category) were:

- *It’s already secure/ Have systems in place/ We’ll ensure security (unspecified)*
- *Issue passwords/ Password protection/ Codes for access*

#### **4.25 Future Impact of New Federal Privacy Laws on Businesses**

Respondents were asked to indicate the extent to which the new Federal privacy laws would impact on businesses: *As far as you are aware, to what extent will these new privacy laws impact upon the way your business is conducted?* The distribution of responses to this question is shown in Table 69. Note that only those respondents

who stated that their organisation had a high level or some knowledge concerning the new Federal privacy laws were asked to respond to this question.

**Table 69: Extent of Future Impact of New Federal Privacy Laws on the Way Business is Conducted**

*“As far as you are aware, to what extent will these new privacy laws impact upon the way your business is conducted?”*

<b>Response</b>	<b>Total (250) %</b>
To a large extent	10
To some extent	44
Not at all	43
Can't say	3
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisation had a high level or some knowledge concerning the new federal privacy laws.

Slightly over half the subsample (54%) said they thought the new privacy laws will have an impact upon the way their business is conducted (*To a large extent/ To some extent*). However, a substantial proportion of respondents (43%) said the new privacy laws would *not* impact on the way their business is conducted (*Not at all*).

#### **4.26 Ways that New Federal Privacy Laws Impact on Businesses**

Respondents were asked, *How do you think the new laws will impact on your business?* Responses to this question are shown in Table 70. Note that only those respondents who stated that the new privacy laws would impact on their business to some extent were asked to respond to this question.

**Table 70: Ways That New Federal Privacy Laws Will Impact on Business**

*“How do you think the new laws will impact upon your business?”*

Response	Total (131) %
More work/ Paperwork/ Red tape (e.g. review procedures/ update databases)	24
Moderate/ Not much impact	17
It will be costly to implement	15
We already partly comply	6
Makes us more aware of privacy regulations	6
Staff training will be required	4
More monitoring/ Control/ Staff control	4
We will have to make new declarations/ Inform customers of the new laws	4
It will be beneficial/ It is positive/ Improve business	4
It will limit the amount or type of data we can collect	4
It will influence the way we collect/ Keep data	4
Inconvenience of having customers wanting to see their files	2
Negative impact/ It will limit us/ Disruptions to business	2
Makes businesses more aware of their responsibility regarding privacy	2
We will have to comply/ We would always comply	2
It will close us down	0
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who stated that the new privacy laws would impact on their business to some extent.

The most common reasons (representing over 10% of responses in each category) given for the new Federal privacy laws impacting on business were:

- *More work/ Paperwork/ Red tape*
- *Moderate/ Not much impact*
- *It will be costly to implement*

#### 4.27 Organisational Preparation for New Legislation

Respondents were asked to indicate whether their organisations had started preparing for the new legislation: *Has your organisation started preparing for the new legislation yet?* Responses to this question are shown in Table 71.

**Table 71: Organisational Preparation for the New Legislation**

*“Has your organisation started preparing for the new legislation yet?”*

Response	Total (560) %
Yes	19
No	61
No, not aware	13
Can't say	7
Total	100

*Base: All respondents.*

A large majority of the sample (74%) said their organisation had *not* started preparing for the new legislation. Less than 20% of the sample (19%) said that their organisation *had* started preparing for the new legislation.

The pattern of responses to the question about organisational preparation for the new legislation was generally consistent across industry groups (see Table 72).

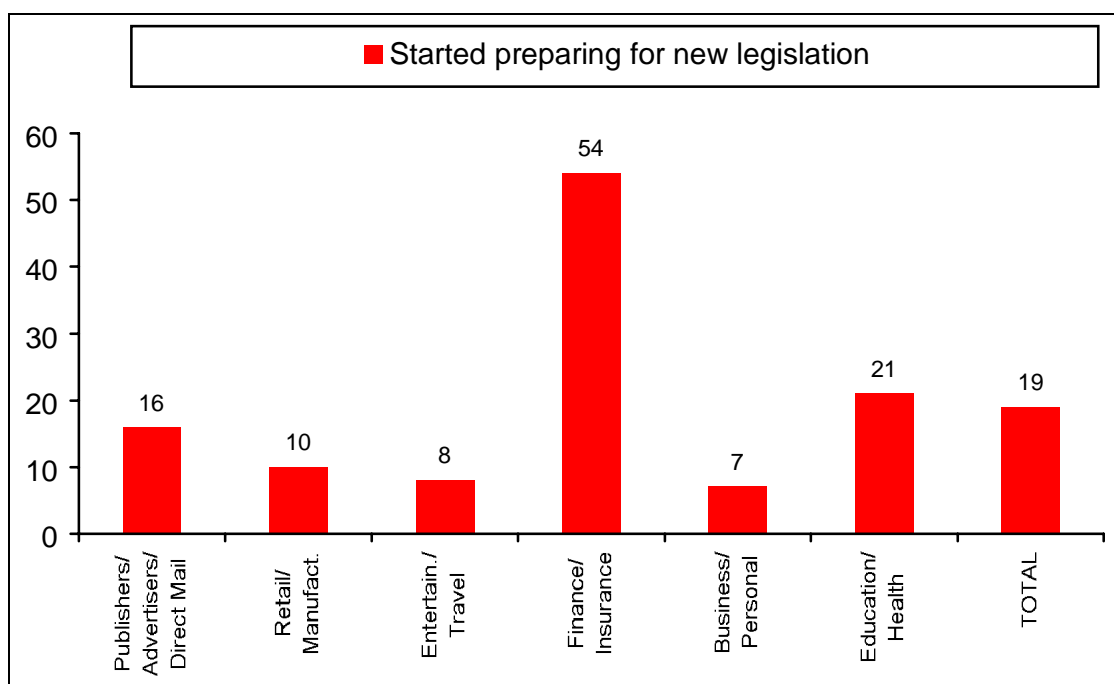
**Table 72: Organisational Preparation for the New Legislation by Industry**

Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(92) %	(135) %	(73) %	(82) %	(84) %	(94) %
Yes	16	10	8	54	7	21
No	68	70	60	28	75	57
No, not aware	8	16	25	9	10	15
Can't say	8	4	7	9	8	7

The large majority of respondents in each industry group (range 72% to 86%, except Finance/Insurance, 37%) said their organisations had *not* started preparing for the new legislation. The exception to this pattern is in the Finance/Insurance sector, where 54% of respondents said their organisation *had* started preparing for the new legislation (see Figure 21).

**Figure 21: Organisational Preparation for the New Legislation**

*“Has your organisation started preparing for the new legislation yet?”*



Organisational preparation for the new legislation seems to vary by the size of the organisation and whether the organisation has a privacy officer (see Table 73).

**Table 73: Organisational Preparation for the New Legislation by Size of Organisation and Location of Privacy Officer**

Response	Size of Organisation		Privacy Officer in Organisation	
	< 20 Employees	≥ 20 Employees	Has Privacy Officer	No Privacy Officer
	(315)	(245)	(199)	(361)
	%	%	%	%
Yes	11	29	34	10
No	70	50	50	67
No, not aware	12	15	11	15



Can't say	7	6	5	8
-----------	---	---	---	---

Most respondents (82%) in organisations with less than 20 employees said their organisations *had not* started preparing for the new legislation, as did the majority (65%) of respondents in organisations with more than 20 employees. However, a substantial proportion (29%) of respondents in larger organisations said their organisations *had* started preparing for the new legislation.

The majority (82%) of respondents in organisations without a privacy officer as well as the majority (61%) of respondents in organisations with a privacy officer said that their organisations had not started preparing for the new legislation. However, a considerable proportion (34%) of respondents in organisations with a privacy officer said their organisations had started preparing for the new legislation.

Organisational preparation for the new legislation seems to vary by the size of the organisation and whether the organisation has a privacy officer (see Table 74).

**Table 74: Organisational Preparation for the New Legislation by State**

Response	VIC	NSW	QLD	WA
	(164) %	(188) %	(74) %	(61) %
Yes	25	18	9	15
No	57	56	76	70
No, not aware	12	15	7	15
Can't say	6	11	8	0
Total	100	100	100	100

*Base: All respondents in specified States.*

The responses suggest that the two larger states (Victoria and New South Wales) are more prepared for the new legislation than the smaller states.

#### **4.28 Sufficiency of Information to Prepare for New Legislation**

Those respondents who stated that their organisations had not started preparing for the new legislation were asked: *Do you believe you have sufficient information on the new privacy laws to begin preparing for the new legislation?* Responses to this question are shown in Table 75.

**Table 75: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation**

“Do you believe you have sufficient information on the new privacy laws to begin preparing for the new legislation?”

<u>Response</u>	<u>Total (341) %</u>
Yes	6
No	91

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisations had not started preparing for the new legislation.

A large majority (91%) of respondents who said their organisations *had not* started preparing for the new legislation believed that they did not have sufficient information on the new privacy laws to begin preparing for the new legislation; only 6% said they *had* sufficient information on the new legislation to start preparation.

This pattern of responses was generally consistent across industry groups (see Table 76).

**Table 76: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation by Type of Industry**

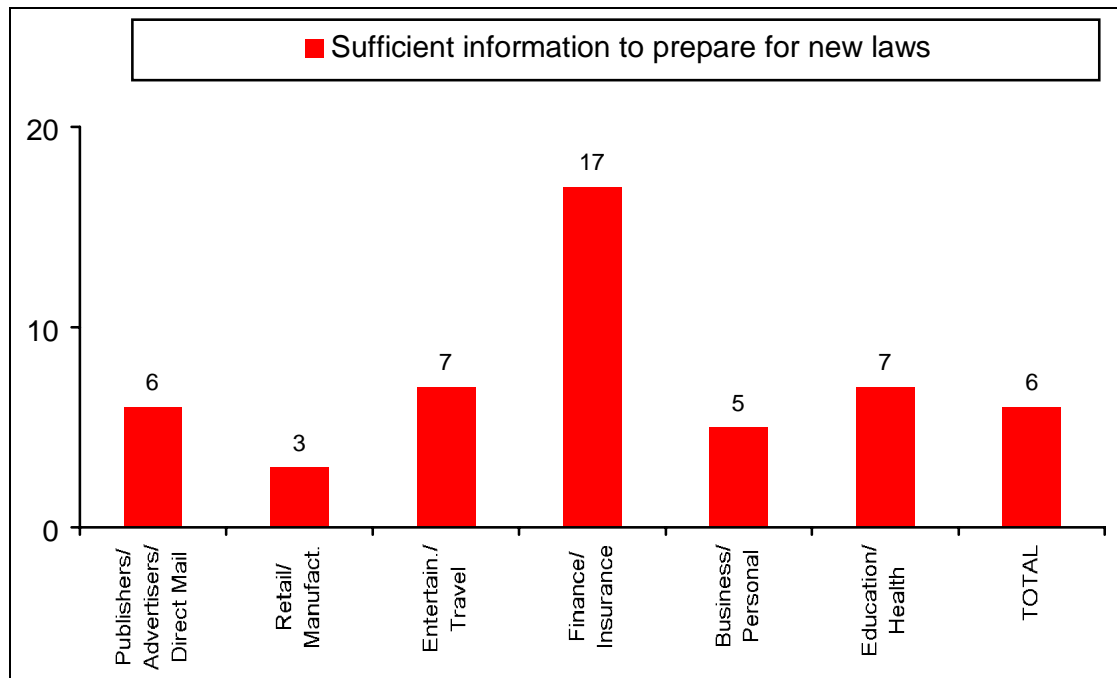
<u>Response</u>	<u>Publishers/ Advertisers/ Direct Mail</u>	<u>Retail/ Manufact</u>	<u>Entertain/ Travel</u>	<u>Finance/ Insurance</u>	<u>Business/ Personal Services</u>	<u>Education/ Health</u>
	(63) %	(94) %	(44) %	(23) %	(63) %	(54) %
Yes	6	3	7	17	5	7
No	90	95	89	83	90	89
Can't say	4	2	4	0	5	4
Total	100	100	100	100	100	100

*Note:* The figures in the table refer to a subsample of respondents: those who stated that their organisations had not started preparing for the new legislation.

Most respondents (range 83% to 95%) in all industry groups said they *did not* have sufficient information on the new privacy laws to begin preparing for the new legislation. Only one industry sector, Finance/Insurance, had more than 10% of respondents stating that they *did* have sufficient information to begin preparing for the new legislation (see Figure 22).

**Figure 22: Sufficiency of Information on New Privacy Laws to Prepare for the New Legislation**

*“Do you believe you have sufficient information on the new privacy laws to begin preparing for the new legislation?”*



#### 4.29 Barriers to Organisational Compliance With New Legislation

Respondents who stated that their organisations had some knowledge concerning the new laws were asked, *What barriers or potential barriers, if any, do you believe there are for your organisation in terms of complying with the new legislation?*

Responses to this question are shown in Table 77.

**Table 77: Potential Barriers to Organisational Compliance with New Legislation**

*“What barriers or potential barriers, if any, do you believe there are for your organisation in terms of complying with the new legislation?”*

Response	Total (241) %
Lack of information/ Need more information	7
Cost of staff education and training	6
Cost of updating technology systems	5
Time taken to implement the new laws/ Update systems/ Reporting to Government	5
Legal costs	2
Cost of updating security systems	2
Education/ Awareness programs/ Employee awareness	2
Re-designing printing materials	1
Lack of knowledge about legislation	<1
Lack of resources (staff)	<1
Burden on Human Resources	<1
Re-designing websites	<1
Not relevant/No impact	5
No barriers	63
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who said their organisations had some knowledge of the new privacy legislation. Respondents could give more than one response.

Note that the majority (63%) of the sample said that there were *no barriers* for their organisations in terms of complying with the new legislation.

The most commonly cited barriers (representing more than 5% of responses in each category) to organisational compliance were:

- *Lack of information/ Need more information*
- *Cost of staff education and training*
- *Cost of updating technology systems*
- *Time taken to implement the new laws/ Update systems/ Reporting to Government*

### 4.30 Sources for Further Information About New Privacy Laws

Responses to the question, *Who would you contact in order to obtain further information on the new privacy laws?* are shown in Table 78.

**Table 78: Possible Sources to Contact for Further Information About New Privacy Laws**

*“Who would you contact in order to obtain further information on the new privacy laws?”*

Response	Total (435) %
Industry Association	30
Privacy Commissioner	23
Solicitor/ Lawyer	11
Government/ Government Department (State or Federal)/ Government Printery	10
Internet/ Website (unspecified)	5
Internally (e.g., Manager/ Head Office)	4
Appropriate Government Body/ Agency/ Organisations (unspecified)	4
Local Government/ Council/ Local MP	2
Government Website	2
Accountants	2
Office of Fair Trading/ Minister of Fair Trading	2
Department of Consumer Affairs/ ACCC	2
Chamber of Commerce (Federal or Local)	1
Union	1
Management Consultants	1
Total	100

*Note:* Respondents could give more than one source.

The most commonly cited sources (representing more than 10% of responses) to contact for further information about the new privacy laws were:

- *Industry Association*
- *Privacy Commissioner*
- *Solicitor/ Lawyer*
- *Government/ Government Department/ Government Printery*

The next most frequently cited sources (representing about 5% of responses) for information were:

- *Internet/ Website (unspecified)*
- *Internally (e.g., Manager/ Head Office)*
- *Appropriate Government Body/ Agency/ Organisations (unspecified)*

#### **4.31 Awareness of the Office of the Federal Privacy Commissioner**

Those respondents who did not mention the Office of the Privacy Commissioner as a source of information about the new privacy legislation were asked: *Were you aware of the Office of the Federal Privacy Commissioner before this interview?*

Responses to this question are shown in Table 79.

**Table 79: Awareness of the Office of the Federal Privacy Commissioner**

*“Were you aware of the Office of the Federal Privacy Commissioner before this interview?”*

<b>Response</b>	<b>Total (455) %</b>
Yes	36
No	64
Total	100

*Note:* The figures in the table refer to a subsample of respondents: those who did not mention the Office of the Privacy Commissioner as a source of information about the new privacy legislation.

The majority (64%) of respondents who had not mentioned the Privacy Commissioner as a source of information about the new legislation said they had *not* been aware of the Office of the Federal Privacy Commissioner before the interview. However, a

substantial proportion (36%) of this subsample had heard of the Office of the Federal Privacy Commissioner.

This pattern of responses was generally consistent across industry groups (see Table 80).

**Table 80: Awareness of the Office of the Federal Privacy Commissioner by Type of Industry**

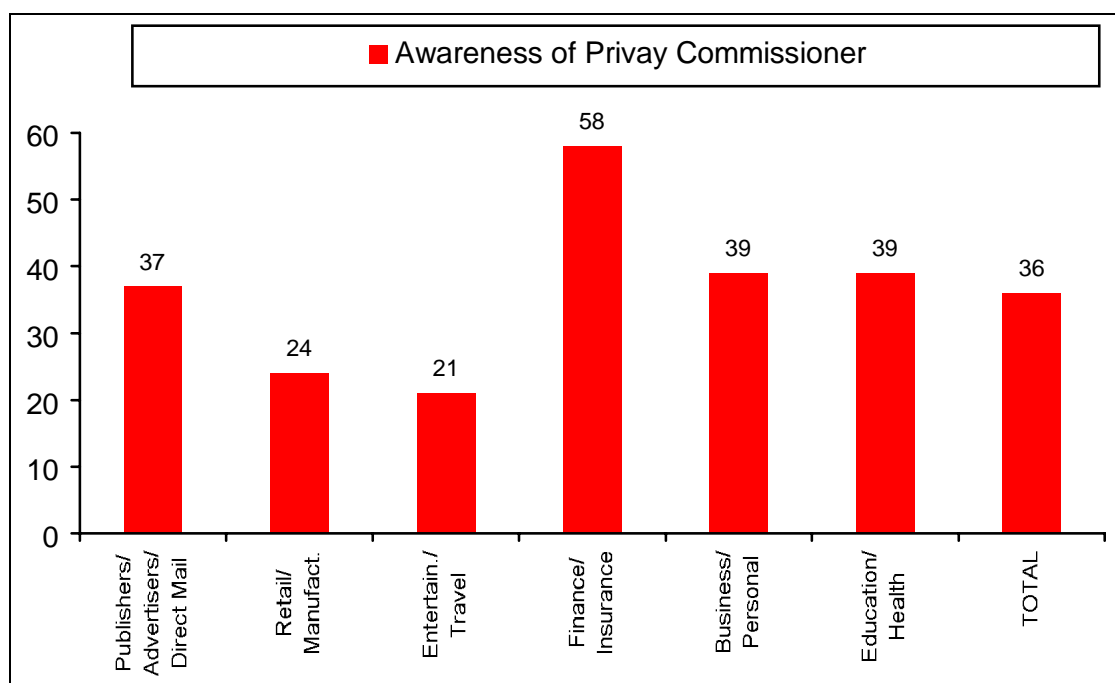
Response	Publishers/ Advertisers/ Direct Mail	Retail/ Manufact	Entertain/ Travel	Finance/ Insurance	Business/ Personal Services	Education/ Health
	(73) %	(115) %	(61) %	(64) %	(72) %	(70) %
Yes	37	24	21	58	39	39
No	63	76	79	42	61	61
Total	100	100	100	100	100	100

*Note:* The figures in the table refer to a subsample of respondents: those who did not mention the Office of the Privacy Commissioner as a source of information about the new privacy legislation.

The majority (range 61% to 79%) of respondents in all industry groups (except Finance/Insurance, 42%) said they had not known about the Office of the Privacy Commissioner prior to the interview. The industry sector that seems to have better awareness of the Office of the Federal Privacy Commissioner is Finance/Insurance; the majority (58%) of respondents in this group said they were aware of the Office of the Federal Privacy Commissioner before the interview (see Figure 23).

**Figure 23: Awareness of the Office of the Federal Privacy Commissioner**

“Were you aware of the Office of the Federal Privacy Commissioner before this interview?”



#### 4.32 Assistance From the Office of the Federal Privacy Commissioner to Organisations

Respondents were asked: *In what ways, if any, could the Office of the Federal Privacy Commissioner assist your organisation to prepare for the amended privacy laws that come into effect in December?* Responses to this question are shown in Table 81.



**Table 81: Ways that the Office of the Federal Privacy Commissioner Can Assist Organisations to Prepare for Amended Privacy Laws**

*“In what ways, if any, could the Office of the Federal Privacy Commissioner assist your organisation to prepare for the amended privacy laws that come into effect in December?”*

Response	Total (537) %
More information	72
Training for staff	6
Support to Industry Associations	4
Simplify the information/ Language/ Point form summary/ Concise outline	4
Workshops or seminars	4
Website/ On-line information/ E-mail	3
More publicity/ Public relations/ Advertising about the new laws	3
Hotline services	2
A list of consultants and organisations that offer privacy services	1
Explain it within the context of our industry	1
Money	<1
Access to other organisations also covered by the legislation	<1
Total	100

*Note: The figures in the table refer to a subsample of respondents: those who said their organisations had some knowledge of the new privacy legislation. Respondents could give more than one response.*

The most common answer to this question, representing 72% of responses, was:

- *More information*

All other suggestions represented less than 10% of responses in each category.