1-1-2001

Privacy on the internet : Investigation into corporate privacy policy of Australian large private sector organisations on the internet

Keiko Sato

Edith Cowan University

Privacy on the Internet:

Investigation into Corporate Privacy Policy of Australian Large Private Sector Organisations on the Internet

By

Keiko Sato

Master of Business (Management of Information Systems)

Faculty of Business

Edith Cowan University, Western Australia

Date of Submission: September 1999

ABSTRACT

The popularity of the Internet has been dramatically increased over recent years. The rapid growth of this technology and its international use has made it almost impossible to regulate the Internet. As a result, the Internet has certainly provided freedoms to people and it has led to some abusing systems.

Privacy is one of the major issues in the development of Electronic Commerce using the Internet. As an enormous amount of personal information is transmitted to several hosts connecting to the Internet, the information can be accessed by both authorised and unauthorised people. Although it is certain that there are several existing problems of using the Internet for business activities, many organisations have already started using it. It is believed that the Internet provides efficiency and effectiveness for various activities

Although much research has been described the business use of the Internet in many countries, these studies have not specifically investigated Australian organisations. Therefore, this research investigates the current use of the Internet by Australian organisations and their associated privacy policies, as a mean of seeking their privacy concerns. Using a benchmark provided by Australian privacy commissioners, it evaluates their privacy policies to see how well they are established to protect privacy of users.

The study utilises the top 100 Australian large private sector organisations as the sample. The current practice of the sample organisations on the Internet was observed by exploring their Web sites. Privacy policies were also collected from their Web sites. Moreover, a letter requesting corporate privacy policy was sent to each organisation that collects personal information on the Internet.

The result showed that the majority of Australian organisations were using the Internet today, but a surprisingly few organisations showed their privacy policy on the Internet. Also, this research showed that many organisations did not actually have a corporate privacy policy. Many organisations are using the Internet without apparent concern for customers' privacy. The organisations proactively involved in the Internet

Commerce are more concerned about security side of the Internet. Hence, they appear to believe that the technology itself protects information sent on the Internet.

It has become clear that technology by itself does not provide the security needed for users of the Internet as unethical act of authorised parties could harm privacy of individuals. There is an argument that the Internet needs to be regulated. However, the process of international regulation on the Internet has not been started. Thus, it is ideal that organisations proactively protect clients' personal information accessible by the use of the Internet technology. This study looks at the methods of obtaining privacy of individuals and suggests the ideal conduct of organisations.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

1) incorporate without acknowledgement any material previously submitted for a degree or diploma in any institution of higher education;

2) contain any material previously published or written by another person except where due reference is made in the text; or

3) contain any defamatory material.

Signature

Date 31 JULY 2001

ACKNOWLEDGEMENT

With gratitude I wish to acknowledge the inspiration and support I have received from several people. Without them, this research would not have been possible.

The advice and encouragement I have received from Dr William Hutchinson, the academic supervisor during the conduct and completion for this research, were greatly appreciated.

Also I would like to acknowledge Associate Professor Dieter Fink who has supported me during the preparation of this research.

I thank the participants of organisations under study who provided their extremely busy time for this research. This thesis would not have been completed without their willingness to share their experiences.

I wish to thank my family and friends who provided me with the emotional support and encouragement, and always believed that I would make it possible.

TABLE OF CONTENTS

CHAPTER ONE

CHAPTER TWO

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

LIST OF TABLES

LIST OF FIGURES

FIGURE **PAGE**

ABBREVIATION

ASIO	Australian Security Intelligence Organisation
CERN	Centre Européen de Recherché Nucléaires
CSCW	Computer Supported Corporative Work
DES	Digital Encryption Standard
S/MIME	Secure Multipart Internet Mail Encoding
EC	Electronic Commerce
EDI	Electronic Data Interchange
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IGIS	Inspector General of Intelligence and Security
IPPs	Information Privacy Principles
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
OECD	Organisation for Economic Co-operation and Development
PGP	Pretty Good Privacy
RSA	Rivest, Shamir, Adlemen
SET	Secure Electronic Transactions
SSL	Secure Socket Layer
SHTTP	Secure HTTP
SMTP	Simple Mail Transfer Protocol
SNMP	Standard Network Management Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
VANs	Value Added Networks
WWW	World Wide Web

CHAPTER ONE

INTRODUCTION

This chapter provides the background of the study and discusses the significance of this research. Then, the purpose of this research is described. The research questions to be answered in this study are also stated in this chapter. At the end of this chapter, the structure of this thesis is described and shows how these questions are answered.

Background Of The Study

Electronic Commerce (EC) is the way of conducting businesses electronically (Zgodzinkski, 1997; Clarke, 1997d). EC in business applications has expanded beyond Electronic Data Interchange (EDI). EDI comprises the standards and services that allow companies' computers to perform electronic transactions without human intervention (Radosevich, 1996). EDI messages are understandable to everyone who has the capability of EDI, that is, EDI standards, EDI software and third party providers such as Value Added Networks (VANs) (Emmelhainz,1990). EDI has been proved to be reliable by many large organisations regardless of its high costs in implementing EDI, especially its cost of using VANs (Emmelhainz,1990; Jilovec, 1997; Ratnasingham, 1998a). Its high costs limit the number of participants of small organisations (Lacovou et al., 1995; Baum, 1996; Ratnasingham, 1998a). Therefore, EDI has been the primary method of conducting on-line business-to-business commerce.

The lack of EDI capability of small organisations has been a serious problem in terms of the economy, however, the idea of the replacement of VAN with the Internet has increased the possibility for not only small organisations but also individuals (Gore, 1996; Tucker, 1997; Ratnasingham, 1998a; Streeter et al., 1996).

The Internet may improve EC by bringing down the boundaries that restrict potential participants in EC.

The economic potential of using the Internet is significant. However, the rapid growth in this technology and its international use have made it almost impossible to regulate. The unregulated world of the Internet has certainly provided many opportunities to behave in ways not available to many before. It has also provided a medium to express ideas to a wide audience. This has led to some abusing the system and producing a wide range of criminal and unethical acts. Privacy is one of the major issues in the development of EC using the Internet, because an enormous amount of personal information is transmitted to several hosts connecting to the Internet, and the information can be accessed by both authorised and unauthorised people.

It has become apparent that technology itself does not secure the Internet. There is an argument that the Internet needs to be regulated. However, the process of international regulation on the Internet has not been started. Thus, it is ideal that organisations proactively protect their clients' personal information accessible by the use of the Internet technology. Organisations have started to publish their privacy policies on the Internet stating how personal information collected is treated by them. However, it is uncertain that all organisations are approaching this problem proactively. This research investigates the Internet usage of Australian organisations and their associated privacy protection concerns.

Significance Of The Study

This research will be of interest to a number of groups as follows:

- The organisations under study can see their roles concerning privacy when conducting businesses on the Internet. This could improve their current practices;
- Other organisations on the Internet could clarify their roles in conducting business on the Internet and improve their activities;

- Organisations that are not using the Internet can learn the problems and successes associated with privacy issues on the Internet and learn their expected roles in conducting business using this medium;
- Internet users can reconsider the use of services provided by various organisations on the Internet by learning their concern on privacy issues;
- Government will find the current practice of organisations on the Internet and they can improve Internet environment by providing them a proper use of the Internet; and
- Academics will find some aspects of business on the Internet conducted by Australian organisations that can direct further research.

Purpose Of The Study

The purpose of this research is firstly to clarify the potential business use of the Internet and privacy protection methods on the Internet gleaned from previous studies. Although much research has been described the business use of the Internet in many countries, these studies have not specifically investigated Australian organisations. Thus, it investigates the current use of the Internet by Australian organisations and their associated privacy policies. Then it evaluates these policies to see how well they are established to protect privacy of users by using a benchmark provided by Australian Privacy Commissioners.

Research Questions

This research attempts to ask three major questions:

1. Are Australian organisations participating in the Internet, if so, to what extent do they use it?
2. Does it publish its privacy policy on the Internet or show concern for privacy protection?
3. How well is the privacy policy on the Internet established: does it meet the benchmark, 'National Principles for handling of Personal Information'?

Structure of the Thesis

This introductory chapter provided the background into this research and discussed the significance of this research. The purpose of this research and the research questions directing this study are stated.

Chapter 2 presents a comprehensive review of the literature on the Internet and the issue of privacy on the Internet. It describes Internet technologies and the World Wide Web, and identifies business use of the Internet. Privacy is also defined and privacy issues on the Internet are described. The methods of its protection are further examined to identify.

Chapter 3 describes the research methodology utilised in this research. The sample selection method (which ensures that the sample represents the population), the research design techniques (which ensure that the needed information is collected efficiently and effectively), the process of data collection, and data analysis techniques used in this study are described in this chapter.

Chapter 4 presents the results of the data analysis in response to the information obtained from the observation and surveys. Research questions are reviewed and discussed in details. The limitations of the research are described at the end of chapter, as the results obtained in this research must be viewed in understanding these limitations of this research.

In conclusion, Chapter 5 discusses implications for organisations, users, and EC. At the end of this thesis, the recommendations for future research are stated.

CHAPTER TWO

LITERATURE REVIEW

Chapter 2 presents a comprehensive review of the literature on the Internet and the issue of privacy on the Internet. To understand why the Internet is used for business purposes, firstly, this section describes Internet technologies and the World Wide Web (WWW, Web). Secondly, it describes the business use of the Internet for organisations and its advantages. Then, the definition of privacy is given. Privacy issues on the Internet are described with supported examples. The methods of privacy protection that are gleaned from previous studies are described at the end of this section.

The Internet and World Wide Web (WWW, Web)

The Internet began in the 1970s as an academic computer science experiment funded by the U.S. Department of Defence (Clarke, 1998b; Lynch and Rose, 1995). The Internet is now referred to as an open network by which the community of people and organisations all over the world are capable of communicating with each other (Lane and Summerhill, 1993; Dahl and Lesnick, 1996; Clarke, 1998b). Clarke (1998a) describes the Internet as a mesh of computer networks that transmit messages to one another using a set of rules that govern the communications, namely protocols. The family of protocols that implement the Internet is referred to as TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP was published as a standard in 1983. Collin (1997, p.29) describes a number of important benefits that leads to its world wide use:

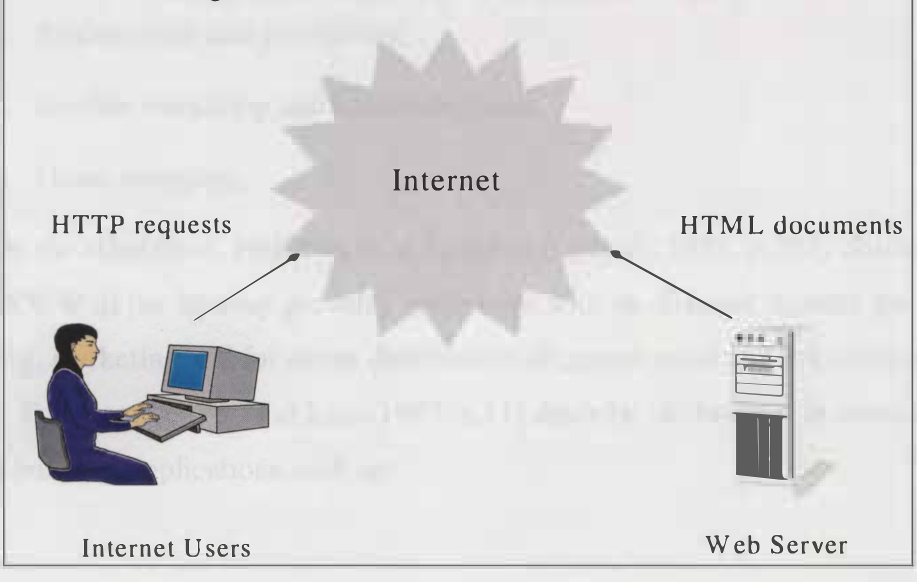
- ❑ It runs on a wide range of hardware;
- ❑ It works on different computer platforms and operating systems;

- It is an open standard that is not owned by any manufacturer; and
- It can route data via a particular route to reduce traffic or to bypass a faulty link.

The use of TCP/IP has been also increasing within closed networks such as Intranets, which are networks within individual organisations, and Extranets, which are networks among closely knit associations of organisations (Clarke, 1998b). However, the Internet, that is further described, does not include such closed networks.

The Internet's capabilities are expansive. One part of the Internet that is of great importance is the WWW. That is, a hypermedia information retrieval system that originated from the CERN (Centre Européen de Recherches Nucléaires): the European particle physic laboratory located in Geneva, Switzerland (Rubin et al., 1997). It is organised as a set of HTTP (HyperText Transfer Protocol)/WWW servers designed for distribution of hypermedia documents. Hypermedia language used to construct WWW pages is called HTML (HyperText Markup Language). HTML defines formatted text, images, audio, video, clips, fill in forms, hyperlinks to other HTML documents and Internet resources. The WWW allows everyone who has access to the Internet to publish any information regardless of its purposes without going through a publisher (Clarke, 1998b). Its ease of use has increased the number of people who publish information on various kinds of topics. How the WWW works is shown in Figure 2.1. Clients with a browser that allows to view

Figure 2.1: How A Web Server Works



WWW pages send requests to web servers that understand and act on the request. A requested WWW page appears on clients' screen within a short time.

The other parts of the Internet include FTP (File Transfer Protocol) for file transfer, SMTP (Simple Mail Transfer Protocol) for e-mail transfer, Telnet to control a remote computers, and SNMP (Standard Network Management Protocol) for network management. The capabilities of the Internet are beneficial for a wide range of people and the number of people taking advantages of this technology is increasing dramatically every year (Senn, 1995; Forcht and Wex, 1996; Renton, 1997; Ng et al., 1998). Many organisations or individuals have started using it for business and others are considering using it. The next section describes the business use of the Internet in details.

Business Use of the Internet

In the past, the Internet was primarily for research, government and education institutions. Today, many researchers have described the potential business use of the Internet. Some consider the Internet as the replacement of VAN eliminating the high cost of conducting EC. Kalakota and Whinston (cited in Nath et al., 1998) described EC applications as follows:

- ❑ Supply chain management;
- ❑ Video on-demand;
- ❑ Remote banking;
- ❑ Procurement and purchasing;
- ❑ On-line marketing and advertising; and
- ❑ Home shopping.

On the other hand, Hoffman et al. (cited in Ng et al., 1998, p.293) claimed that the WWW of the Internet provides companies with an efficient channel for advertising, marketing and for direct distribution of certain good and information services. Furthermore, Foo and Lim (1997, p.11) describe the Internet in terms of potential business applications such as:

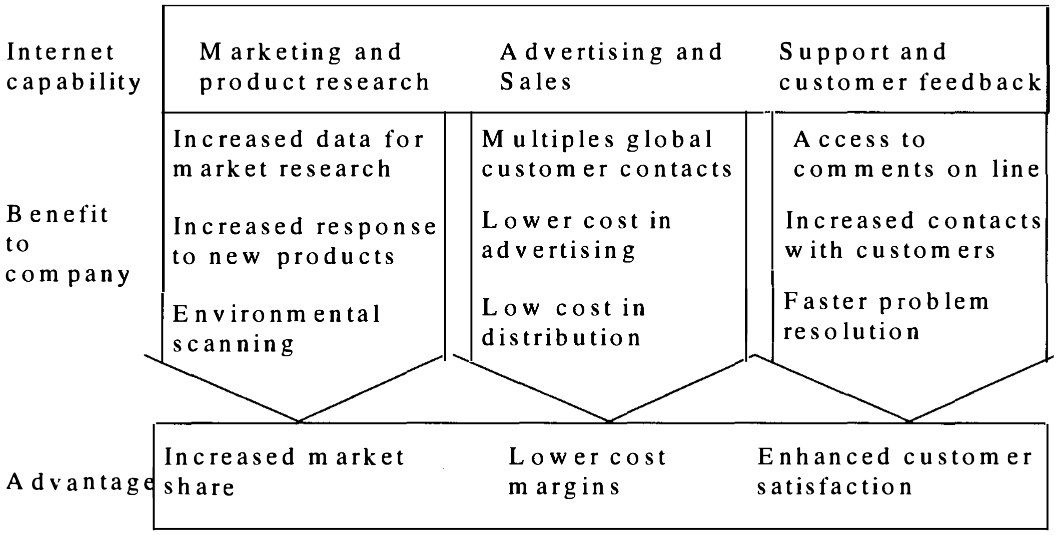
- A public relations tool to establish a global presence and heighten public interest;
- A marketing tool to advertise goods and services and to open up international markets;
- A marketplace to sell good and services;
- An information kiosk to provide latest business information, frequently asked questions and time sensitive information;
- An alternative support tool to answer customers' queries and solicit feedback;
- A research or information gathering tool for market surveys, product launches and obtain solutions to problems encountered from around the world;
- A human resource tool for recruitment;
- A support tool to serve mobile employees; and
- A Computer-Supported Corporative Work tool (CSCW) to facilitate group work and communication internally and externally.

These studies have described much of all potential business use of the Internet. Cronin (1995) simplifies the above Internet capabilities as well as its advantages using Michael Porter's value chain. Cronin's Internet value chain examines its relationship with suppliers, customers, and internal operations. These Internet value chains provide a clear view of the Internet for business but it should be pointed out that the Internet enables suppliers to contact customers directly, hence, the way of doing business will likely to be changed with its use. Thus, in this study, the Internet value chains are modified and examines its relationship with customers and internal operations. The following summarises the potential business activities on the Internet as well as its advantages described by the above authors.

Customer Relationship

Organisations aim at achieving competitive advantages. An important factor to competitive advantages is to achieve customer satisfaction (Cravens, 1994). Thus, the customers' needs and wants are the foundation of business. The Internet capabilities that improve customer relationship are classified into three as follows. (see Figure 2.2)

Figure 2.2: Internet Value Chain: Customer Relationship
(modified - Cronin, 1995)



Internet capability	Marketing and product research	Advertising and Sales	Support and customer feedback
Benefit to company	Increased data for market research Increased response to new products Environmental scanning	Multiples global customer contacts Lower cost in advertising Low cost in distribution	Access to comments on line Increased contacts with customers Faster problem resolution
Advantage	Increased market share	Lower cost margins	Enhanced customer satisfaction

Marketing and product research

Continuous market research is vital to obtain information about customers in a changing environment. "Thousands of discussion groups and bulletin boards are available for keeping in touch with new developments through environmental scanning, as well as for direct contact with customers." (Cronin, 1995, p.61) In the past, companies were unable to obtain customers' personal information without having them filling out a form. Today, WWW servers can automatically save personal information of customers who visit virtual shops without the customers' knowledge. Companies could then use this information for further market analysis.

Also, information-gathering tools enable researchers for market surveys, product launches, and even to obtain solutions to problems encountered around the world (Foo and Lim, 1997).

Advertising and sales

The most common business use of the Internet today is for advertising. The Web technology enables to publish a huge amount of information on the products/services/companies in interesting images to global customers who are interested in them. Companies are competing with each other by differentiation of products and services (Cravens, 1994). Angelides (1997) stated that selling on the Web is one of the vehicles of choice in creating differentiation sales activities because clients are offered to buy cheaper products by eliminating normal expenses of running a retail store such as rent, electricity, and reducing the number of human resources. Products such as books, software can be transmitted through the Internet in a short time. Thus, it eliminates the cost of packaging, postage fees as well. They can be distributed at any time of customers' convenience by offering 24 hours, 7 days and shop from home. In addition, clients are allowed to easily pay by credit card, smart cards (McElroy and Turban, 1998), e-cash and other devices.

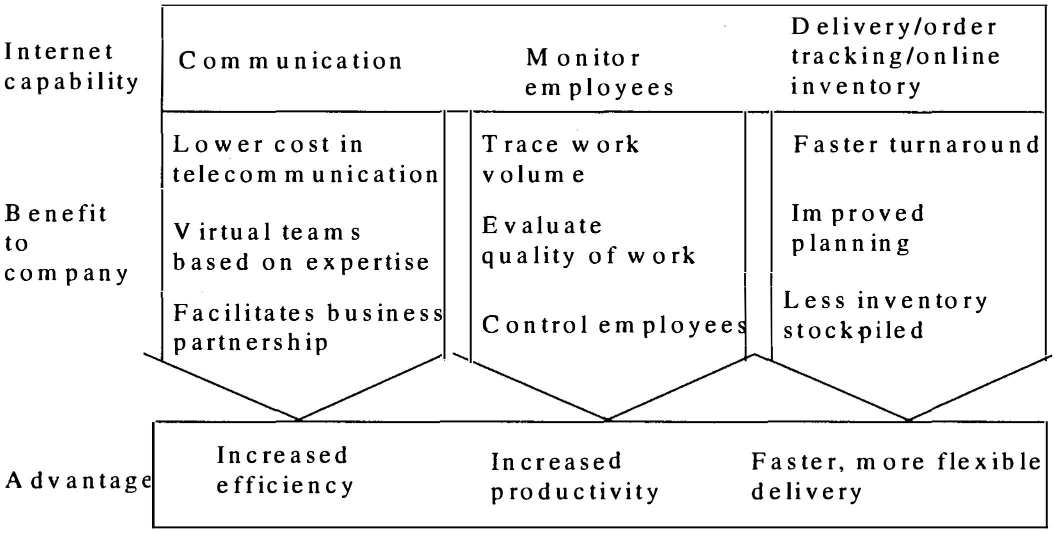
Support and customer feedback

Well-organised Web sites provide the best service by allowing clients an easy access to a specific product/service/information. Clients would not waste time in searching it, hence, it eliminates clients' frustration. Emails can also be used to send updated information to global customers and/or to support customers. Providing good customer service is one of the most important roles of organisations. Traditional customer services make clients wait for a long time in line or on hold, and then often redirect to other person for a short query. On-line customer support eliminates such frustration of customers by providing a faster problem resolution. Most customers solve their problems by viewing the 'frequently asked questions' site. This site multiplies customer contacts without incremental costs. If a particular problem was unsolved, they can contact customer service by an e-mail that allows a representative to prepare the answer and reach the customer. This can be done at both parties' convenience. Combination of one-to-one communication, fast and accurate service is likely to provide the best service to customers.

Internal Operations

On the other hand, the massive amount of information organised by computing technologies has already improved many ways of managing internal operations. The capabilities of Internet technologies have furthermore improved many areas of business operation within organisations (Cronin, 1995; Streeters et al., 1996). (see Figure 2.3)

Figure 2.3: Internet Value Chain: Internal Operations
(modified – Cronin, 1995)



Internet capability	Communication	Monitor employees	Delivery/order tracking/online inventory
Benefit to company	Lower cost in telecommunication Virtual teams based on expertise Facilitates business partnership	Trace work volume Evaluate quality of work Control employees	Faster turnaround Improved planning Less inventory stockpiled
Advantage	Increased efficiency	Increased productivity	Faster, more flexible delivery

Communication

The Internet has improved communication methods. Traditional internal communication methods included memoranda and telephone, while external communication included telephone, facsimile and mail. With the Internet, e-mail, video-conferencing, chatting are added to both of internal and external communication methods with lower costs and faster access.

Today, employees can work from home with just a connection to the Internet. Companies normally advertise positions in newspaper, recruiting books, and education institutions, and they have been recruiting people based on their location up to date. However, the Internet eliminates the recruiting costs by allowing companies to advertise job vacancies on their Web sites. Also it allows companies to build virtual teams based on expertise (Cronin, 1995). It will be possible for many organisations to utilise the networking marketing structure with the use of the Internet. Employees can be paid on the basis of their sales/work volume that can be traced and measured using the monitoring capability of the Internet.

Monitor Employees

The capabilities of Internet technologies allow managers to monitor employees who use companies' facilities (Lawrence, 1998). The work that employees do can be traced by the use of this technology. This includes all the sites they visit, all the e-mails they send and receive, every conversation made on the Internet, and any documents sent or received on the Internet. "..., much of the popular literature on computer-based monitoring stresses the negative effects of monitoring on workers, no matter how or where it is implemented." (George, 1996, p.459) It seems that monitoring is often seen as too onerous or invasive. (see Data Confidentiality) However, it could be argued that a well-implemented monitoring system motivates employees to increase their productivity and to improve the quality of their work. Management has a key role to play in designing an effective monitoring system that is not only to benefit them but also to motivate employees (George, 1996).

Delivery/online tracking/online inventory

Finally, on-line tracking of orders and inventory improves inventory control, and less inventory needs to be stockpiled. Also, keying orders can be done only once among all parties by using electronic documents. It eliminates the re-keying activities, thus, it can reduce data entering errors and delays.

To take full benefits of this technology, many organisations have started using it for various purposes. Also many individuals have started new businesses on the Internet. The rapid growth in technologies and its international usage are making it almost impossible to regulate the Internet environment. As a result, a wide range of criminal or unethical acts is capable of being performed. Today, privacy has been called one of the most important ethical issues associated with the Internet technologies. (Culnan, 1993; Smith, 1993; Clarke, 1997c; Washburn and Tauber, 1997). In the next section, privacy is defined.

Definition of Privacy

The word *privacy* stems from the Latin word *privatus*, which literally means "apart from the public life" (Bacard, 1995, p.34). Clarke (1997b, p.2) defines privacy as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations." Stone (1983, cited in Smith et al., 1996) defines information privacy as "the ability of the individual to personally control information about one's self". On the other hand, Agranoff (1991, p.48) defines information privacy in terms of three issues:

- ❑ Data Collection – personal data should be gathered for only relevant and legitimate purposes;
- ❑ Data Accuracy – individuals should have the right to access and correct personal data on stored files; and
- ❑ Data Confidentiality – The individual should have the right to know who has access to personal data and have the opportunity to approve its disclosure to others.

Some information on a person should not be exposed to public scrutiny, hence, protection of personal information should be considered along with further development of the Internet. Thus, in this study, privacy is defined as:

> *The personal space where individuals are able to keep their personal information away from others.*

The term, personal information, is often used in this research, thus it is further described in the following section.

Personal Information

> *"Personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. (Privacy Commissioner, 1995)*

There are a number of ways in which personal information can be gathered and processed on the Internet. Dwyer (1994) categorises personal information in computerised networks into three dimensions:

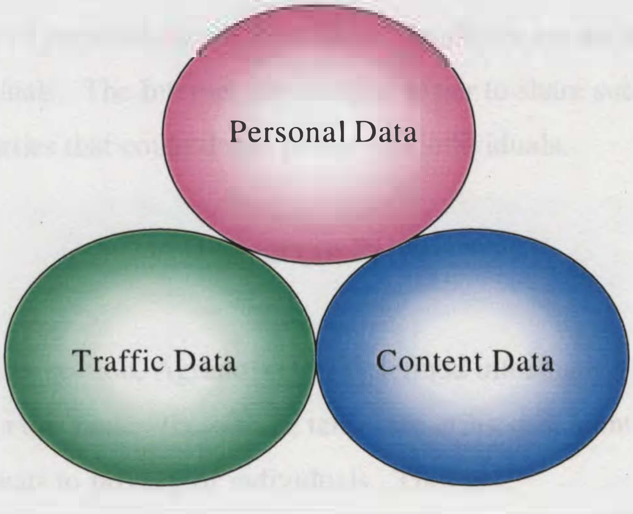
- Customer information;
- Traffic data; and
- Content data.

Clarke (1997b) describes four dimensions of private information in a similar manner:

- The person's body;
- Behaviours;
- Communications; and
- Data about themselves.

The person's body can be visualised on the Internet and it can be treated as data about themselves. Also behaviours on the Internet can be described by tracing every site a person visited and every word they typed. Communications can be described by monitoring communication software such as e-mails, video conference and chatting. They identify the person who are communicating with and conversation or messages sent between them. In classifying these data, three categories are constructed in this study as shown in Figure 2.4. The definitions of each category are described as follows:

Figure 2.4: Personal Information on the Internet



Personal Data

This category of information is information that required submitting when filling an application form including names, addresses, and other personal details. It may also include education, job histories, financial information, credit card number, photo and so on. Personal data allows the provision of service for billing purposes and to prevent or detect fraud for organisations.

Traffic Data

Traffic data means information captured automatically by computers on usage of communication networks. It includes a number of communications made, duration of the communication with destination details. Traffic data is kept and allowed calculation of the usage of communication networks for billing purposes.

Content Data

Content data includes the conversation or messages made during the communication. On-line communication between two parties is no longer personal as anyone on-line can listen to it with or without one's intention. Content data is often used to discover one's thoughts on various subjects and/or to detect criminal conducts on communication networks.

The exposure of the above data can result in threats to privacy of individuals (Hochheiser, 1996; Washburn and Tauber, 1997). Computers are seen as the major threat to privacy issues, in fact, in 1994, more than 70 percent of Australians felt that computers were reducing the level of privacy in Australia (O'Connor, 1995). Massive amounts of personal data in centralised databases are no longer under control by individuals. The Internet has made it easier to share such information among several parties that could threat privacy of individuals.

Threats to Privacy

In the earlier section, Agranoff (1991) defined information privacy in terms of three issues. In this paper, these three terms are utilised in identifying several issues seen as threats to privacy of individuals. They are:

- ❑ Data Collection;
- ❑ Data Accuracy; and
- ❑ Data Confidentiality.

Data Collection

Personal information should be gathered for only relevant purposes and should not be used for other purposes. However, it is often used for secondary purposes without authorisation from individuals. That is, personal information is often re-used only to fulfil business purposes. For example, once you provide your personal data to apply for a credit card, the marketing department of the bank often uses the information to offer you other services such as loans and investments. Similarly, telecommunication companies use traffic data not only for billing purposes but also for marketing purposes. As an example, a person who often makes calls to the USA receives letters from telecommunication companies stating that they offer a cheaper rate. Also the person receives a call from a machine of a telecommunication company saying, "I know that you make calls to USA often, we would like to inform you that we offer cheap rates to USA." It seems that every call made is monitored and used by telecommunication companies for marketing purposes. Although these marketing activities may not be considered as threats to one's privacy, an increased re-use of personal data may well be. In fact, personal data is often shared by several organisations. For example, a person who applied for a subscription of a computer magazine starts receiving letters advertising other magazines from different publishers. In this case, it is clear that the personal information was passed to the other publishers. When credit card numbers are also passed and used by the other organisations, it is recognised as a crime. However, when other personal data is reused, it is not considered as a serious problem. The increased value of information is attracting organisations to gather personal data and use without authorisation from individuals. Organisations such as direct marketing industries are claimed to be threatening privacy today (Culnan, 1993).

Data Accuracy

Data stored in organisational databases have a significant rate of errors (Kelin and Goodhue, 1997). However, society often expects that the information stored in corporate databases is accurate. An incorrectly entered personal information can cause great emotional and financial damage (Bologna, 1991). For example, banks would decline your personal loan if you have a large amount of debt stored in credit record inaccurately. Also, your job application would be unsuccessful if a criminal conviction has been incorrectly entered against your name. Operational errors in handling personal data often occur either deliberately or accidentally (Smith, 1993).

Smith (1993) describes that accidental errors are mistakes such as data entry mistakes occur without one's intention, while deliberate errors are intentional misreporting of information. That is, incorrect information is entered purposely, often for one's benefits. For example, Head (1998) described common computer crimes associated with deliberate errors: "data diddling" and "salami slicing". "Data diddling" is to modify data without authority. "Salami slicing" is to shave a little off every transaction and redirecting it to a third party account.

The definition of accidental errors and deliberate errors can be easily described, however, the determination of whether it is occurred accidentally or deliberately is difficult in reality. In fact, it is often considered as a crime when an error associates with money. On the other hand, if a person deliberately modified personal data of someone such as medical histories, it can be treated as an accidental error.

In addition, it must be pointed out that there are several difficulties in maintaining and ensuring the accuracy of information (Mason, 1986). Firstly, electronic documents have created difficulties in ensuring accurate data. In paper documents, modification made on a document was much easier to detect than that on electronic documents. Modification made on electronic documents often cannot be detected without a proof of printed documents or back up made before modification. Without these proofs, the modified data is determined as an accurate data. Also there will be a tendency to put more information in databases/servers that can result in difficulties of maintaining and ensuring the accuracy of information. In fact, EC may be making easier for an unethical person to conduct various kinds of activities that harm others by creating inaccurate information about them, and leaving them open to public scrutiny.

Any individual who has access to the Internet can publish personal information of individuals (Clarke, 1998b). Privacy of individuals can be harmed easily by publishing secret information or untrue stories. For example, you may find your photo and personal story on a Web page of someone that you do not even know. In the photo, you could be next to someone that you have never seen in your life. The story could be untrue as well. Modified photos can be done perfectly by today's technologies. Everyone is likely to believe that the published information is true. You would not be able to prove that the information is wrong. People all over the world could access to this information once it is published. The Internet has made it possible not only to publish the secret information of individuals but also the incorrect information that harms privacy of individuals. Furthermore, the Internet permits anonymity (Pattison, 1997). The creator of the Web page could be different from the owner of the Web page who claims to be. And it is possible that the owner of the Web page does not know about it. The use of e-mail has the same situation. An unethical employee can send company's secret information using someone's e-mail account so that the person will not be suspected. Threats to individual of privacy exposure and/or being suspected for criminal conducts are great. It seems that the Internet has made it difficult to determine the accuracy of information.

Data Confidentiality

Previous surveys (O'Connor, 1995) showed that confidentiality of personal information is an important issue for most Australians. Data confidentiality closely relates to access to personal information stored in corporate databases. Sipior and Ward (1995) defined access to personal information into two parties: authorised or unauthorised. (see Table 2.1)

Businesses and government organisations are threaten by unauthorised parties such as hackers and/or disgruntled employees who access to a company's computer (Lorek, 1997). Organisations should ideally eliminate unauthorised parties' access by utilising secure technological options. However, the previous report found that 49.0% of computer crimes involved unauthorised access (Head, 1998). Unauthorised access can be easily accomplished by employees exposing the secret information about corporate computer systems to others, or pretending themselves to be unauthorised parties. Thus, personal information is in danger of being misused by authorised parties as well.

Table 2.1: Access to Personal Information

Authorised Parties	Unauthorised Parties
□ Government	□ Hacker, Cracker
□ Organisations	□ Eavesdropper

Authorised parties can be employers, service providers, information providers, information collectors, system administrators, software developers and the government. They handle massive amounts of personal data provided by users to their databases as well as traffic data and content data that travelled from one host to several other hosts on the Internet and stored in several logs automatically (Pattison, 1997). Any authorised people could access information stored in organisation's databases for their own benefits. In Australia, the private sector remains exposed to attack on its information systems by their employees (Head, 1998). If authorised parties treat personal data unethically or insecurely, it can threat privacy of people. Several issues that arise in handling of personal information by authorised parties are described in the followings.

Mason (1986) describes that the computer technologies' enhanced capacity for surveillance, communications, computation, storage, and retrieval is threatening privacy. Several authorised parties grant rights for surveillance or secret searches in order to detect criminal and/or unethical activities on the Internet. They are seeking means of limiting its use for illegal purposes by the use of several new technologies such as video surveillance, data surveillance and so forth. On the Internet, data surveillance technologies are seen as risks to privacy (Shattuck, 1984; Linowes, 1993; Clarke, 1997b). Data surveillance is the systematic use of personal data in the investigation or monitoring of the actions or communications of one or more persons (Clarke, 1997a). Four data surveillance techniques are further described by Clarke (1997b) as follows:

- ❑ Front-end Verification – the cross-checking of data in an application form, against data from other personal data systems;
- ❑ Computer Matching – the expropriation of data maintained by two or more personal data systems;
- ❑ Profiling – the classification of person from past experience, and data-holdings;
- ❑ Data Trail - a succession of identified transactions.

Also, as briefly described in the earlier section, employers utilise computer monitoring systems to investigate traffic data as well as content data in order to observe employees' every conduct on corporate communication networks. The case often brought up by the use of this kind of data is that, a employee who sent an e-mail to his co-worker criticising his supervisor was fired. Organisations remain their right to monitoring their property. Thus, every call you made on the company's phone, every e-mail you sent from work could be monitored by the employers. Such monitoring is certainly threatening privacy of employees. However, it could be argued that such tool is necessary for organisations to detect criminal and/or unethical behaviour of employees. The monitoring of employees is widely taken place in Australia (Wearne, 1998). As a result, the monitoring tools such as WebSpy detected, in a big WA company, only 45 percent of the traffic going across its Internet connection was business related, and 75 percent of employees are unethically visiting work unrelated web sites during work: employees were using the corporate Internet account to visit sexually explicit, chat, sport and hobby web sites (Wearne, 1998). Traffic data is not only used for tracking one's activities but also used to examine interests and relationship with other parties. Collected data is stored onto databases and enable to create a "digital persona", a model of an individuals' public personality (Clarke, 1994). Such monitoring are also conducted by government to detect criminal activities of citizen.

In Australia, wire-tapping telephone conversations and/or reading contents of messages on the Internet were prohibited and Australian government authorities generally respect these prohibitions (Clarke, 1998b). However, in early 1999, Australian Security Intelligence Organisation (ASIO) was given legal access for the first time to financial transaction and tax records, and the ability to hack into sites

(Barker, 1999). Also law enforcement agencies of other countries are able to eavesdrop on other allied countries' telephone and cable traffic via a network of listening stations. (Available at http://www.privacy.org.html)

Personal information is vital for government to detect criminal activities of citizen and for business to detect unethical behaviours of employees. However, individuals should have control over their personal information and some information of personal nature should be able to keep away from the public eye (Culnan, 1993). Hence, protection of personal information should be carefully examined. In the next section, it looks at how privacy can be protected in Australia.

Protection of Privacy

The majority of Australians believe that it is governments' responsibility to protect their privacy, hence, Australians require privacy laws to apply to both government and business (O'Connor, 1995). However, laws and regulations themselves would not protect privacy in reality. Garfilkel and Spafford (1997) identified three approaches in protecting personal information:

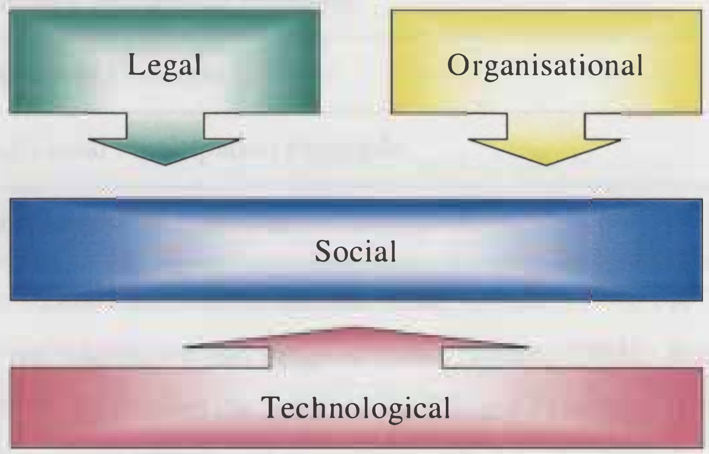
- Secure personal information in the server;
- Secure personal information that travels between the server and the user; and
- Secure personal information stored in the user's computer.

Also, technical and legal forms of protecting personal information are described by Rotenberg (1993) as follow:

> *"Technical forms seek to reduce the risk of interception of communication, unauthorised access to records of communications, or to conceal the identities of the parties to a communication. Legal forms establish rights that are enforceable in law."*

On the other hand, Weisband and Reinig (1995) suggested that organisations should manage user perceptions of email privacy, which can be influenced by an understanding of technological, managerial and social factors. They will learn through their experience and education to be aware of the privacy risks. For example, passwords are fallible so anyone can possibly look through their conduct, and system administrators can access their account if they like to. Secondly, the lack of management policies reinforces the perception that no one is watching. It is necessary to ensure that policies are established and implemented in the right way. Finally, it is stated that social norms directly influence the organisation's use of email and affect its use of other communication media. This paper combines the two and classifies protection of privacy into four approaches. (see Figure 2.5) Each level of protection is described in the following sections.

Figure 2.5: Privacy Protection Model



Legal Approach

To date, Internet technologies and services have been largely unregulated (Straub and Collins, 1990; Ford, 1996; Clarke, 1998b). However, there are some regulations developed to protect privacy of people (Shattuck, 1984; Laudon; 1996; Privacy Protection in the Private Sector, 1996; Clarke, 1997b; Privacy Commissioner, 1998).

In 1978, the Organisation for Economic Co-operation and Development (OECD) were made up of two dozen countries including much of Europe, the U. S., Canada, Japan, and Australia, promoting several international guidelines to develop EC through a variety of commercial applications, to bolster user confidence in networks, and to provide for data security and privacy protection (OECD, 1997, URL: http://www.oecd.org.)

Eight information principles included in the OECD guidelines are shown in Table 2.5.

Table 2.2: The OECD Principles 1978

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Due to technological developments since the late 1970s, the OECD guidelines do not address the full range of issues (Dixon, 1995). Australia as a member of OECD introduced the Information Privacy Principles (IPPs) in the Australian Privacy Act 1988 based on guidelines for the protection of privacy and transborder flows of personal information that were developed by the OECD. Eleven principles in IPPs are listed in Table 2.3.

Privacy Act 1988 deals primarily with the information handling practices of Commonwealth and Australian Capital Territory (ACT) government agencies. There is no similar legislation in any state or the Northern Territory (NT), although the South Australian, West Australian and Tasmanian governments have drafted IPPs to apply to their own handling of personal information. Also New South Wales and South Australia have Privacy Committees that assist in fair handling of personal information. (Privacy Commissioner, n.d.) On the other hand, current Commonwealth Law provides privacy protection in the area of tax file numbers, consumer credit reporting, spent convictions, data-matching, Medicare and pharmaceutical benefits, and medical research (Clarke, 1996). In fact, the private sector has remained almost unregulated by privacy and data protection legislation (Dixon, 1995).

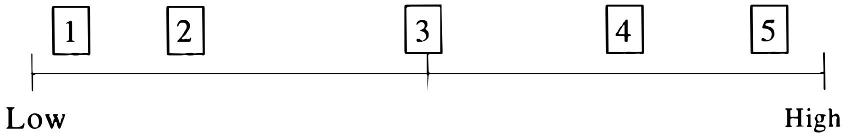
Table 2.3: Privacy Act 1988: Information Privacy Principles

1. Manner and purpose of collection of personal information
2. Solicitation of personal information from individual concerned
3. Solicitation of personal information generally
4. Storage and security of personal information
5. Information relating to records kept by record-keeper
6. Access to records containing personal information
7. Alteration of records containing personal information
8. Record keeper to check accuracy etc. of personal information before use
9. Personal information to be used only for relevant purposes
10. Limits on use of personal information
11. Limits on disclosure of personal information

The study of Milberg et al. (1995) clarified global regulatory approaches of corporate privacy management classified in five models (see Figure 2.6).

It shows Regulation Models that differ in the level of government involvement. In Australia, government is involved in corporate privacy management by assigning the Privacy Commissioner to help Australian Businesses to develop

Figure 2.6: Regulation Models by Smith (1994)
(cited in Milberg et al., 1995)



1 Self Help Model depends on data subjects' challenging inappropriate record keeping practices.

2 Voluntary Control Model relies on self-regulation on the part of corporate players.

3 Data Commissioner Model relies on the ombudsman concept through a commissioner's office.

4 Registration Model creates a requirement that each databank must be registered.

5 Licensing Model creates a requirement that each databank containing personal data be licensed.

voluntary codes of conduct to meet privacy standards.

In February 1998, the Privacy Commissioner issued "National Principles for the Fair Handling Personal Information" (Scollay, 1998). This represents the first stage in the development of a national privacy scheme for Australia. These principles have been framed in general terms so that they may be applied to personal information held by a wide range of organisations. Ten principles contained in this scheme are listed in Table 2.4.

Also, in New South Wales, the Australian Privacy Charter Council has brought together a wide range of experts to establish a clear statement of the meaning of the right to privacy for Australians, and to spell out principles to guide organisations and individuals in observing this right. The Privacy Charter was launched in 6 December 1994 as a set of privacy standards of both the public and private sectors (Clarke, 1996; The Australian Privacy Charter, n.d.).

Table 2.4: National Principles for Fair Handling of Personal Information

1. Collection
2. Use and Disclosure
3. Data Quality
4. Data Security
5. Openness
6. Access and Correction
7. Identifier
8. Anonymity
9. Transborder Data Flows
10. Sensitive Information

Principles included in Privacy Charter are listed in Table 2.5. Many principles in the Privacy Charter are based on the IPPs of Privacy Act 1988. This Privacy Charter was designed to address the technologies of the 1990s and beyond, without the limitations of being technology-specific. The Council believes that the private sector should not wait for the passage of legislation to take measures to protect the privacy of employees and customers (Dixon, 1995). Thus, the organisational approach to privacy protection is examined in the next section.

Table 2.5: The Privacy Charter

1. Justification & Exceptions
2. Consent
3. Accountability
4. Observance
5. Openness
6. Freedom from surveillance
7. Privacy of Communications
8. Private Space
9. Physical Privacy
10. Anonymous Transactions
11. Collection Limitation
12. Information quality
13. Access & Correction
14. Security
15. Use and Disclosure limitations
16. Retention limitation
17. Public registers
18. No disadvantage

Organisational Approach

Organisations handle a wide range of personal information of both their employees and users. As stated earlier, it is ideal that organisations establish a privacy policy in order to standardise conducts of employees in handling of personal information, and to notify clients and users how personal information collected from them is used. Unfortunately, it seems that many organisations do not act on this matter.

Several studies have been conducted to approach privacy issue by investigating organisational practices. Smith (1993) examined information privacy issues by conducting semi-structured interviews with 105 executives and managers in seven organisations: three insurance organisations, three banks and one credit card issuer, that deals with sensitive personal information. It addressed both the process of crafting information privacy policies as well as the current policies and practices in the organisations. Further, the surveys were distributed to 1103 employees of four participating organisations addressing their view of mismatches between policy and practice. The results showed that most organisations acknowledged of having poor privacy policy, however, do not respond to this matter unless external threats pressure them to. And their employees have no 'upsetting' experience with their company's use of personal information, though employees have limited factual knowledge about the types of personal information and its use by their companies, and about their companies' policies.

Later, Smith et al. (1996) developed and validated a parsimonious 15-items instrument with four sub-scales tapping into four primary dimensions of individuals' concerns about organisational information privacy practices:

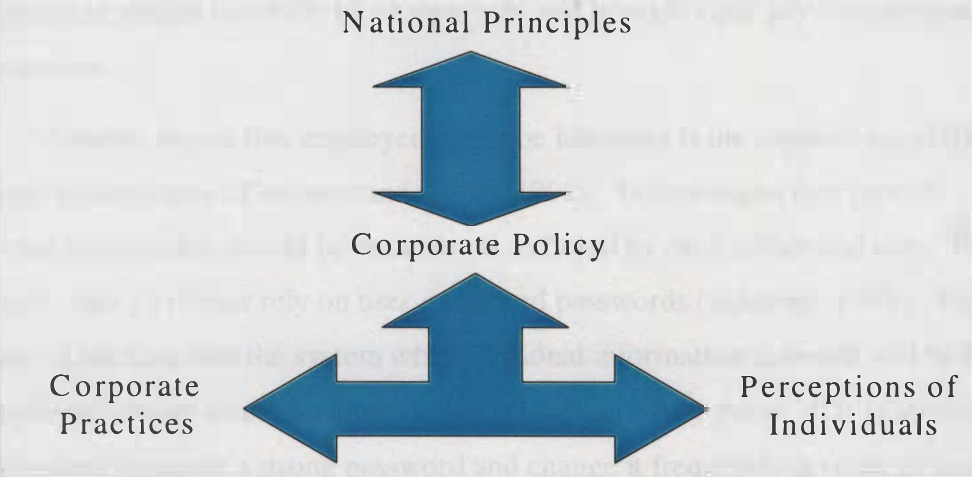
- Collection;
- Error;
- Secondary use; and
- Improper access.

The above items were identified as the most central dimensions of individuals' concerns about organisational information privacy practices in this study. This instrument can serve as the first step on a path of proactive management to guide organisations to a better practice in handing personal information (Smith et al., 1996).

On the other hand, Culnan (1993) examined individuals' attitudes toward secondary use of information such as direct marketing practices only. The results showed that people who are less sensitive about secondary use of personal information have positive attitudes toward direct marketing and have developed ability to cope with unwanted mail.

From these previous studies, it has become clear that organisations can provide privacy protection concerning three main factors: corporate policies, corporate practices, and individuals' perceptions of these practices (see Figure 2.7). That is, Information privacy can be facilitated by establishing and implementing a well established corporate privacy policy, and informing individuals the policy to perceive positive corporate practices. A maximum level of privacy protection can be provided by organisations when three dimensions match while the corporate policy meets the National Principles for Fair Handling of Personal Information.

Figure 2.7: Organisational Approach to Privacy Protection



Guidelines to establish good corporate policies are described in the earlier section. Thus, the establishment of good corporate policies should be easily accomplished by following those guidelines and contacting the Privacy Commissioner. Also, individuals' perceptions can be only controlled by informing individuals their policies (Woodman et al., 1982). In the following, corporate practices are described.

As each employee's conducts represent organisational practices, it is difficult to standardise corporate practices. However, it is ideal that organisations educate employees in both the ethical and technical aspects of the Internet usage in order to standardise employees' conduct.

Organisations develop policies and codes in various areas to control employees' conduct (Lichtenstein and Swatman, 1997). However, these policies and codes are seen as written documents that established and filed. For example, codes of ethics, documents showing the organisations' commitment to values and ethical conduct expected from its employees, are employed by many organisations today (Kling, 1996). However, the study of Harrington (1996) on the effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions showed that they do have an effect but they are related to only certain abuses. The study concluded that organisations could expect codes to have some impact if they take responsibility to notify employees of corporate policies and codes, but they can not expect to control employee behaviours solely through codes of ethics. Thus, the use of formal/informal penalties, and/or incentives are recommended to be in use to support such policies. It is also suggested that management should carefully hire employees and provide clear job descriptions and expectations.

Another aspect that employees must be informed is the capabilities of the Internet technologies (Thomson and Solms, 1998). Technologies that protect personal information should be understood and used by each authorised user. For example, many systems rely on user-generated passwords (Schneier, 1998). The chance of hacking into the system where personal information is stored will be high if employees create an easy password that others can easily guess. It is essential to inform users to create a strong password and change it frequently in order to avoid others from guessing their password, especially if the person has an authorisation of access to valuable data of the organisations.

Finally, the Internet capabilities of monitoring employees were briefly described in the earlier section. Computer-based monitoring has a bad reputation, however, companies must ensure that employees are working as expected. The study of George (1996) explored employees' perception of computer-base monitoring. The results showed that computer based monitoring is used in a punitive manner and contributes to work-related stress and illness but management can also manipulate the system not to be invasive but in a way that increased pressure to produce can affect work quality. Managers are claimed to be threatening privacy of employees. The act of logging on with a password may lead users to think their work can not be accessed by anyone other than themselves. Similarly users may think that deleted documents cannot be accessed by other without knowing the capability of storing backups of deleted documents (Weisband and Reinig, 1995). The role of managers and the use of monitoring tools should be clearly specified by the top management (Wolinsky and Sylvester, 1992). Also employees' understanding of these technologies help verify their perception of privacy. Although monitoring tools are threatening privacy of employees, it is essential for organisations to ensure ethical conduct of each employee. Because unethical conducts of employees are threatening companies as well as clients. Thus, technological approach to privacy protection is essential to organisations.

Technological

In seeking ways of protecting privacy at technological level, firstly, five foundations of information security defined in ISO 7498 –2 should be pointed out (cited in Foo et al., 1999):

1. Data Integrity - Data should not be changed after it is sent;
2. Confidentiality - Data should be viewed only by the person who created it or its recipients;
3. Access Control – Data should be viewed only by the person who has the authorised access;
4. Authentication - Data received should be from the people it claims to be from; and
5. Non-repudiation - Data having sent by a person should not be refused by the sender.

Not one device covers all five attributes to protect privacy (Foo et al., 1999). The combination of the above tools secures the data stored in server and users' computer, and the data that travels on the Internet. Thus, a combination of several technologies should be considered to provide a high level of information security.

A number of technologies are available in today's market to secure information. Gartner Group, an IT consultant company, breaks the security market into 12 segments:

1. Access Control;
2. Anti-Virus;
3. Assessment;
4. Certification;
5. Cryptography;
6. Enhanced User Authentication;
7. Firewalls;
8. Logging;
9. Reporting;
10. Alerting;
11. Physical Security; and
12. Secure, Consolidated User Authentication.

The consensus among security experts is that companies need five tools after establishing a security policy to adequately protect IT infrastructures (Rutrell, 1998).

- ❑ Encryption – protects the confidentiality of critical data that traverses over private and public enterprise networks;
- ❑ Firewalls – guard an enterprise network from security breaches that stem from outside the company via the Internet connections;
- ❑ Authentication/authorisation – let administrators grant and control access privileges to computing resources by users, departments and services;
- ❑ Anti-virus - Scan for and take corrective action against malicious viruses that enter corporate networks through the Internet links; and
- ❑ Intrusion-detection – monitor networked devices to ferret out security holes.

"One of the primary methods to protect communications privacy is cryptography." (Rotenberg, 1993) Cryptography is an important element in transmitting and storing personal information requirements. It is the practical art of converting messages or data into a different form so that no one can read them with out having access to the "key" (Clarke, 1998c). The key allows the person in possession of the message to decode it. Two different key encryption schemes are the private key and the public key.

The private key scheme relies on the existence of a single, secret key that is used both to encrypt and decrypt messages. Therefore, private key encryption makes it necessary first to exchange the key used to encrypt messages between the sender and each recipient. As it uses only a single key to encrypt and decrypt, it is impractical, inefficient. And private keys lack in security when users communicate a large number of people all around the world. Also, the fact that multiple parties know the key implies that authentication by means of knowledge of the key becomes very difficult, and non-repudiation issues are almost impossible to address when any one in the group could edit or reply messages in transit from the source to the intended recipient (Foo et al., 1999). The example of private key encryption includes Digital Encryption Standard (DES) by the US government.

On the other hand, public key scheme involves two related keys, public key and private key. Public key is published so that anyone can use it to encrypt a message and a related private key is used to decrypt a message. The examples of public key encryption are RSA (Rivest, Shamir, Adlemen) developed by three mathematicians, PGP (Pretty Good Privacy) by Phil Zimmermann, SSL (Secure Socket Layer) by Netscape, SHTTP (Secure HTTP) by NCSA (developer of the concepts of the Web), SET (Secure Electronic Transactions) introduced by Visa and MasterCard and S/MIME(Secure Multipart Internet Mail Encoding). These are widely used today as they provide data integrity, authenticity, confidentiality, and non-repudiation.

Public key encryption is widely used in other applications. For example, "digital signature" is an application of public key technology (Gluck, 1994). A person creates and attaches unique identifying codes to their documents. It provides integrity, authenticity, and non-repudiation but not confidentiality. Another example is "digital certificates". A digital certificate is issued by the trusted party, Certificate Authorities (CAs) and provides any recipient of a digital signature with a copy of the sender's public key, plus assurance that the public key really belongs to the sender. (Wilson, 1997, p.177) It provides integrity, authenticity and non-repudiation.

Cryptography is an important tool in privacy protection, however, cryptography technologies that cover confidentiality have been restricted by many countries as it allows criminals to send secret communications over public network (Wilson, 1997). With the limitation of its use by government, personal information will never be protected. Also, Garfilkel and Spafford (1997, p.210) describes some problems of cryptography:

□ It can not protect unencrypted original documents still reside in the computer;

□ It can not protect against stolen encryption keys;

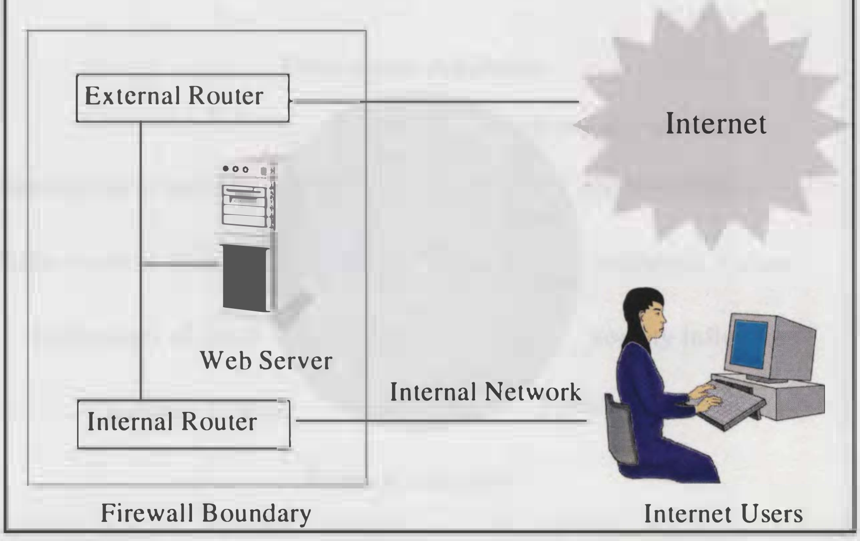
□ It can not protect against denial of service attacks;

□ It can not protect traffic data unless encrypted separately; and

□ It can not protect against encryption program modified by attackers.

Thus, other protection tools must be covered. Encryption can not guarantee the security of the computer if people can break into it. Considering the security of the computer, physical security as well as logical security must be pointed out. The computer as well as the network should be protected by the use of locks, in order to keep them physically inaccessible to unauthorised parties (Foo et al., 1999).

Figure 2.8: Best Practice Firewall Configuration
(Doddrell, 1995)



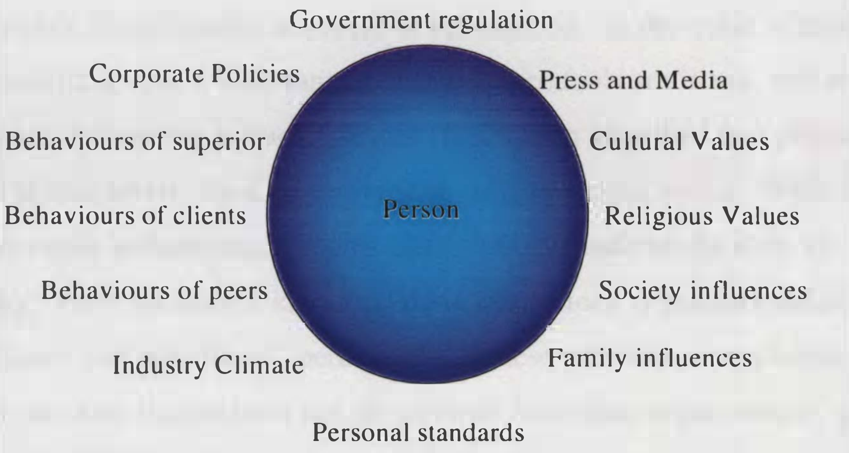
On the other hand, a firewall is a logical barrier that provides some protection for corporate information from the Internet or other network (Doddrell, 1995). A firewall is a hardware device or software application that looks at all the raw data transferred to the server from the public Internet. It blocks unauthorised parties from getting into the server and blocks data that damages the server such as mail-bombs, or viruses. Figure 2.8 shows best practice firewall configuration. This protects the server and provides some confidentiality to data stored in the server.

The described technological approaches restrict access to servers, users' computers and networks by examining the user ID and matching password or keys. The technological approaches can be easily failed when unethical individuals use their authority to view information for their own benefits or when unethical individuals without authority use the Internet to harm privacy of others. Thus, final important factors in privacy protection are individuals' ethical behaviour as well as perceptions of privacy on the Internet.

Social

Social approaches to privacy protection include two issues. Firstly, it tries to control behaviours of individuals. There is a need for Internet users to learn ethical behaviours required on the Internet. Schermerhorn (1992) defined "Ethics" as the system or code of morals of a particular person, religion, group, profession that sets standards as to what is good or bad or right or wrong in one's conduct. Figure 2.9 shows several factors affecting ethics of people.

Figure 2.9: Factors Affecting Ethics
(modified Schermerhorn, 1992)



People build their standards through their experience and education (Weisband and Reinig, 1995). Therefore, the usage of the Internet can be largely influenced by existing Internet users, organisations, government, educational institutions and media. Those parties could proactively influence others to act ethically on the Internet, however, behaviours of individuals are uncontrollable without regulations. Thus, this kind of social approach to privacy protection is not very realistic. Social approach itself does not have power to secure the Internet space. In fact, legal, organisational, and technological approaches to restrict the unethical use of the Internet could largely influence society to act in ethical manner.

On the other hand, social approach could be effective when it is used to adjust perceptions of individuals in privacy protection. If the danger of privacy invasion is informed in advance, people will be more cautious in the use of the technologies. The level of upsetting feeling differs in their expectation/knowledge of its occurrence. That is, informing society the chance of its occurrence and other protection approaches to be provided will adjust individuals' perceptions, and result in a lower level of privacy invasion.

Summary

Internet technologies and the WWW support various activities of organisations especially in marketing and management. The Internet benefits businesses because of its global connectivity, speed, low cost, ease of access, ease of use, flexibility, productivity, equal opportunities that lead to a competitive advantage. On the other hand, a wide range of criminal or unethical acts is capable of being performed: invasion of privacy, inaccuracy of information, breach of property rights, illegal/unethical access to information. In detection of those criminal/unethical acts, a wide range of surveillance tools are in use, and at the same time they are threatening privacy of users. It has been identified that privacy can be protected at four levels: legal, technological, organisational, social. While no privacy legislation exists in Australia, it seems that privacy of individuals is on an uncertainty. Previous studies identified three key factors: organisational policies, their practices, and individuals' perceptions of these practices, in explaining privacy issue. As previous studies have not yet covered Australian organisations' privacy management. This study looks at the first step of privacy management, organisational policies, as stated in second research questions. The next section, research methodology, describes the steps to be taken in this research.

CHAPTER THREE

RESEARCH METHODOLOGY

Different research methodologies and designs will be more or less appropriate depending on the types of questions to be answered (Leedy, 1997). In this section, the research questions are firstly reviewed and the information required to answer these questions are briefly explained and listed. The methodology for this research was designed specifically to reflect these research questions. In the following sections, the research design techniques (which ensure that the needed information is collected efficiently and effectively), and the sample selection method (which ensures that the sample represents the population) are described. The data analysis techniques used in this study are also explained. At the end of this section, the process of this research was summarised.

Review of Research Questions

The nature of the information collected in order to answer each research questions is shown in Table 3.1. The first question of this research was, "Are Australian organisations participating on the Internet, if so, to what extent do they use it?" In addressing this question, the organisations' URL addresses were searched firstly. Once the presence of each organisation on the Internet was detected, their business activities on the Internet were examined by the classifications specifically developed in this research. (see the section: Data Analysis)

The second question of this research was, "Does it publish its privacy policy on the Internet or show concern for privacy protection?" Privacy policy or their privacy concerns shown on the Internet were collected to answer this question. Classifications on the level of their privacy concerns were also developed and explained in the Data Analysis section.

Finally, this research asked, "How well is the privacy policy on the Internet established: does it meet the benchmark, National Principles for handling of Personal Information?" The information collected on privacy policies and concerns shown on the Internet was also used to answer this question.

The information collected from this research, in conjunction with other information from literature review, could describe the current use of the Internet by Australian organisations and their associated privacy policies. It could also guide organisations in the adoption of the Internet for their business activities. However, it must be pointed out that this was a cross-sectional study that was carried out once and represented a snapshot of one point in time. Thus, the results represented only the period of data collection.

Table 3.1: Research Questions and Information Collected

Questions	Information Collected
Question 1 Are Australian organisations participating in the Internet, if so, to what extent do they use it?	□ The URL addresses of organisations to examine their presence on the Internet; and □ Their business activities on the Internet. (Classifications are developed in the Data Analysis section.)
Question 2 Does it publish its privacy policy on the Internet or show concern for privacy protection?	□ Privacy Policy on the Internet or Privacy Concerns shown on the Internet. (Classifications developed in the Data Analysis section.)
Question 3 How well is the privacy policy on the Internet established: does it meet the benchmark, "National Principles for handling of Personal Information"?	□ Privacy Policy on the Internet; and □ Privacy Policy unpublished on the Internet.

Research Design

Although previous studies described the business use of the Internet in many countries, these studies had not specifically investigated into Australian organisations. Therefore, the data needed for this research must be primary data. That is, collected especially to answer the research questions that search current phenomenon not provided by other resources (Zikmund, 1991; Cooper and Emory, 1995).

Basically, there are only two alternatives in collecting primary data: observing conditions, events, people or processes, and questioning, or surveying people about various topics (Cooper and Emory, 1995). For this research, the data can be obtained by either observation or survey methods. However, observation was the central method used to collect the majority of the data required to provide answers to this research because of several reasons described in the followings.

Firstly, observation overcomes many deficiencies of survey by not involving people, respondents. Hence, it eliminates both non-response biases and/or response biases (Zikmund, 1991; Cooper and Emory, 1995; Ghauri et al., 1995). People may refuse an interview or fail to reply to a mail survey. And data can be obtained more accurately through direct observation than by questioning respondents because the data do not have distortions, inaccuracies or other response biases due to such things as memory error (Zikmund, 1991).

Secondly, there are vast areas of information for which observation is the only method available such as the study of records and document analysis/document study (Emory, 1985). In this study, document analysis/document study is the only method available for collecting some data, that is, privacy policies and privacy concerns shown on the Internet.

However, observation method is not bias-free. Accuracy of the data may suffer if the observer adds subjectivity to the recording, called "observer bias" (Zikmund, 1991). As observation method highly relies on the observer alone, the observer must be able to give great attention to details. In supporting the observer (the researcher), a form on which observations are to be recorded should be prepared

(Blank, 1984). Therefore, in order to overcome this limitation, an observation checklist was developed specifically to meet the purpose of observation (see Appendices 1).

Observation method is also limited as a way to learn of the past, intentions, attitudes, opinions and other aspects, which are unable to gain by observing (Emory, 1985). As the purpose of this research is to investigate current phenomenon, observation method provides sufficient information to meet the requirement of this research. However, if an organisation that collects personal information online does have a privacy policy but does not publish it on the Internet, it is the interest of this research. Therefore, unpublished privacy policies on the Internet were requested from such organisations as a mean of understanding their insight.

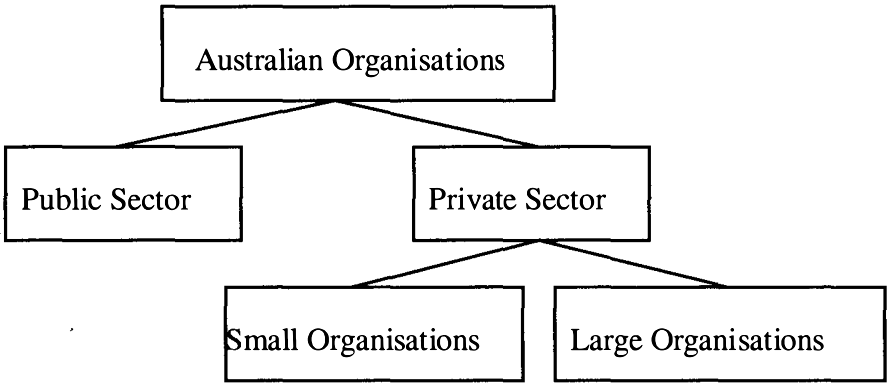
An e-mail was utilised to communicate with organisations in this research for several reasons. Firstly, the sample organisations were located in various states in Australia, and an e-mail was the lowest cost method to collect data. Secondly, people who participate in this research must have great knowledge of their organisations and are preferably involved in the development of their site on the Internet. Such people at the top of the organisations are difficult to reach in any other way, and it was assumed that an e-mail would be a faster way to contact an appropriate respondent. Thirdly, most organisations on the Internet provide an e-mail address for users to contact. Also, a previous study on e-mail use of organisations (Sillince et al., 1998) found that e-mails are the most useful for responding to queries and the volume of external contacts was increased by the adoption of e-mails. It seems that organisations are more contactable using e-mails. Finally, it allows respondents to take more time to consider replies at length than telephone or personal interview. There are more chances to gain valid data by e-mail.

On the other hand, the major weakness of e-mails is non-response biases like survey method. Several techniques in improving mail survey returns described by Cooper and Emory (1995, p.283) were utilised to gain satisfactory response rate. Firstly, follow-ups are suggested to successfully increase response rates. Two weeks after the first e-mail sent, a reminder was sent to each organisation. Secondly, a short questionnaire is suggested to obtain higher response rates. Since this research only aimed to collect their privacy policy that was unavailable on the Internet, a simple letter requesting their privacy policies for the Internet dealing was sent to sample organisations. This letter contained information about the researcher and the purpose of this study (see Appendices 2). However, where e-mail resulted in delivery error, the letter was sent though fax facilities.

Sample Selection

The application of the observation method required selection of sample organisations, as it would be practically impossible to conduct a census of all Australian organisations due to time constraints and limited human resources. "At the outset of the sampling process, it is virtually important to carefully define the target population so the proper source from which the data are to be collected can be identified." (Zikmund, 1991, p.333). Due to the relatively large target population, the population was firstly divided into classes as shown in Figure 3.1.

Figure 3.1: Classification of Organisations



Privacy Act 1988 distinguishes between the public and private sectors. As the Act applies to the public sector only, their policy-making activities may be significantly different from those in the private sector. Whilst the regulation for the private sector regarding privacy issue is still in the process of its completion, a large number of private organisations seem to have expanded their business into the Internet environment. The business conducted on the Internet by such private organisations is mostly unregulated. It is their stated concern for privacy issues that is the interest of this research.

It is estimated 1,046,900 businesses exist in Australia, and this includes 1,004,200 small businesses (less than twenty employees) and 42,700 other businesses (Australia Bureau of Statistic, 1998). (see Table 3.2)

A complete list of population was not accessible. Therefore, a convenient sampling was used. The list of the top 100 private sector businesses in Australia in terms of its revenue published by Australian Business Review Weekly (BRW) Magazine was used in this study, as it was conveniently available.

"The user of research that is based on convenience sample should remember that projecting the results beyond the specific sample is inappropriate." (Zikmund, 1991, p.342) Hence, the sample used in this research could be very non-representative. However, "these problems are less important if the population is highly homogeneous, since there is less opportunity for error." (Kervin, 1992, p.218)

Table 3.2: Number of Businesses in Private Sector

(Australian Bureau of Statistic, 1998)

Industries	Small Businesses	Other Businesses	Total
Agriculture, Forestry and fishing	104,500	12,900	117,400
Goods Producing Industries	239,200	3,100	359,700
Service Industries	660,500	26,700	687,200
Total All Industries	1,004,200	42,700	1,046,900

Deans and Kane (1992, p.19) discuss three components of the external environment: domestic, international and foreign, and also economic, political/legal, cultural/social and technological dimensions of each environment. According to Deans and Kane (1992), four dimensions (economic, political/legal, cultural/social, and technological) can be viewed from a more homogeneous perspective within a domestic environment (one country). Therefore, the population of this research could be homogeneous and the use of convenience sampling could be appropriate in this research.

There were also some specific reasons for using the list of the top 100 private sector not the other lists conveniently available. Organisations develop new policies because of external threats such as *government* and *competitors* (Smith, 1993). In this research, it was assumed that:

- On behalf of the Australian government, the privacy commissioners would have been more likely to contact the top organisations on the issue of privacy on the Internet. The top 100 organisations, as leading organisations in industry, would be the first to react to privacy issues in Information Age; and

- The top 100 organisations' conduct on the Internet is likely to be observed by their competitors. As leading organisations, they have an influencing power to other organisations' business conduct on the Internet. That is, what leading organisations do are more likely to be followed by other organisations in the same industry.

Hence, the chosen sample could be reasonable representatives of the population in order to draw conclusions from the population.

Data Analysis

The data analysis of each collected data is explained in this section. Firstly, it describes the demographic data analysis. Secondly, it explains the classification of business activities on the Internet. Further, organisations are classified depending on their privacy concerns shown on the Internet. Finally, it explains how the collected policies and privacy concerns are analysed.

Demographic Data

As privacy legislation is affecting each industry and each state differently, the type of industries and the location of organisations should be collected. Demographic data were collected from the list provided by the BRW and coded. Coding involves assigning numbers to answers so the responses can be grouped into a limited number of categories (Cooper and Emory, 1995).

The size of organisations were divided into two categories: small businesses (less than twenty employees) and large businesses (twenty or more). The following numbers were assigned to each category:

1. Small businesses; and
2. Large businesses.

The states in Australia were assigned number as follows:

1. New South Wales;
2. Victoria;
3. South Australia;
4. Western Australia;
5. Queensland;
6. Tasmania; and
7. Northern Territory.

The following shows the classifications of industry as used by the BRW with the assigned numbers:

1. Whole sale trade;
2. Retail trade;
3. Manufacturing: food;
4. Construction;
5. Property and business services;
6. Finance and investment;
7. Insurance;
8. Transport and storage;
9. Manufacturing: machinery and equipment;
10. Personal, other services;
11. Health, community services;
12. Manufacturing: printing and publishing;
13. Manufacturing: textiles and clothing;
14. Manufacturing: building materials;
15. Manufacturing: petroleum, chemicals and coal;
16. Manufacturing: metals products;

17. Manufacturing: wood and paper; and

18. Cultural, recreational services.

Business Activities on the Internet

As a coding helps the researcher reduce replies to a few categories containing the critical information needed for analysis, every possible activity was categorised and nominal scale was utilised for measurement. The numbers were assigned to each activity for classification. Many business activities on the Internet were described in previous sections. Kalakota and Whilston (cited in Nath et al., 1998, p.92) articulate a classification scheme for activities that can be accomplished using EC. They are:

- □ Transactions between a company and consumer over public networks for the purpose of home shopping or home banking;
- □ Transactions with trading partners using EDI;
- □ Transactions for information gathering such as market research; and
- □ Transactions for information distribution, including advertising, sales and marketing.

This classification best described the current business activities of organisations, thus it was utilised in this research. However, in addition to this classification, two categories must be added in this research: non-Internet users and under construction as this research conducted on the sample regardless of its participation on the Internet. Therefore, the business activities of organisations on the Internet are classified into six categories:

1. **Non Internet Users**. Do not use the Internet for their business activities. They may use Intranet or Extranet but they are not on the Internet where Internet users can easily access;
2. **Information Providers**. Use the Internet for advertising purposes only. They are on the Internet where Internet users can easily access. They have the facility available on the Internet where Internet users can contact them through e-mail. These companies are able to obtain users' e-mail address and other information that the server automatically saves;

3. **Information Collectors**. Use the Internet for business activities. They have the facility for users to provide their personal information including, name, addresses, contact numbers, and preferences through e-mail;
4. **On-line Traders**. Use the Internet for business trading activities. They have the facility for users to purchase products using credit cards on the Internet;
5. **Restricted Traders**. Use the Internet for business trading activities. These sites can be only accessed by the owner's contracted traders; and
6. **Under Construction**. Will use the Internet for business activities, however, they are still under construction.

The observation checklist (see Appendices 1) provides a clear guideline in classifying sample organisations into each category described above.

Privacy Policy on the Internet

Organisations were further categorised into three classes depending on their privacy statement on their site. The categories were also assigned numbers as below.

1. **No Privacy Policy**. Companies that show no concerns on privacy issues;
2. **Show Concern**. Companies that show their privacy concerns, however, they highly rely on technologies and there is no privacy policy appeared on the Internet; and
3. **Have Privacy Policy**. Companies that provides privacy policy on the Internet

The classified data was entered into SPSS (Statistical Package of Social Science) and frequency tables were produced to display collected data.

Privacy Policies collected on the Internet were evaluated using a benchmark given by the Privacy Commissioner as explained in the earlier section. The National Principle for the Fair Handling of Personal Information were established in February 1998 as to meet international best practice in handling personal information. Using the national principles as guidelines eliminates the researcher's bias and also determines whether Australian organisations meet international best practice in handling personal information.

The following list (see Table 3.3) is an initial guide to the Privacy Commissioner's preferred interpretation of the principles and is used as evaluation criteria in this research. Each privacy policy was examined whether it covered each criterion. Detailed evaluation sheet is available in Appendices 3. This sheet helped the researcher understand meanings of each word that was interpreted by the Privacy Commissioners. The list of categories with its frequency count was produced.

Table 3.3: National Principles

1. Collection
2. Use and Disclosure
3. Data Quality
4. Data Security
5. Openness
6. Access and Correction
7. Identifier
8. Anonymity
9. Transborder Data Flows
10. Sensitive Information

Privacy Concerns Shown on the Internet

Privacy concerns are numerous and varied, therefore, content analysis was used. Content analysis follows a systematic process starting with the selection of a unitization scheme. Cooper and Emory (1995, p.386) claimed that syntactical units are illustrated by words, which are the smallest and most reliable. A number of concerns shown on the Internet are categorised and assigned a numerical score. The categories selected are key words or sentences and a set of categories should be mutually exclusive and contained only one concept dimension (Cooper and Emory, 1995). Although content analysis can be easily done by a computer capturing the words directly from web sites, privacy concerns were analysed by the researcher by counting the word from each criterion on National Principles. Because Webler (1990, p.69) claimed that "...as the opportunity for capturing texts directly from other electronic media increases, the danger of mindless content analysis will also increase." In this research, all samples' privacy concerns were categorised ensuring that they were appropriate, and the list of categories with its frequency count was produced.

Corporate Privacy Policy

Corporate Privacy Policies received from Organisations were analysed using the same method as analysing privacy policies on the Internet described in the earlier section. (see page 45)

Organisations' privacy protection concerns received in surveys were also analysed using the same method as analysing privacy concerns shown on the Internet described earlier. (see page 46)

Procedure

The process of research should be stated clearly step by step so that anyone can follow the conduct of this research (Zikmund, 1991). Therefore, in this section, the steps taken in this research was explained in details.

Firstly, the top 100 private sector businesses were obtained from the list of the top 500 private sector businesses published by BRW magazine (Available at URL: http://www.brw.com.au). The demographic data of the sample was coded and entered into the observation checklist.

In order to enhance reliability of data and to obtain the latest data, the examinations was conducted twice using two different search engines: Australian Yellow Pages (Available at URL: http://www.yellowpages.com.au) and Web Crawler (Available at URL: http://webcrawler.com).

Company names were entered into the search box on each site, and the listed addresses were accessed to ensure that the company under investigation created the site using the following criteria:

1. **Company names**. The name of company matched with the name listed in the top 100 organisations. Or the name was appeared as an owner of the site;
2. **Australian Organisations**. The location of the organisation was in Australia;
3. **Location**. The location of the organisation matched the state of the organisation in the list; and
4. **Industry**. The business matched the industry classified in the list.

The first examination of the top 100 private companies started on 28 August 1998 and finished on 12 September 1998 using the Australian Yellow Pages site. It located sixty-three sites of the top 100 organisations.

The second examination started two weeks after the completion of the first examination. It started on 3 October 1998 and finished on 17 October 1998 using the Web Crawler. It located seventy-seven companies' site on the Internet.

After the second examination, a pattern in the companies' URL addresses were observed, that is, almost all the Australian companies have their Web sites at 'http://www.(company name).com.au.' or 'http://www.(company name).net.au'. As a mean of ensuring the Internet presence of each organisation, 'http://www.(company name).com.au' as well as 'http://www.(company name).net.au' were entered into URL. This search using URL was conducted on the last day of the second search engine search. As a result of this follow-up search, the number of companies located were the same as the result shown by the second search.

Each site was explored to classify their business activities on the Internet as well as their privacy concerns and policies shown on their sites as described in the previous section. When an organisation was classified into either Information Collector or Trader, a letter requesting the companies' privacy policy for the Internet users was sent by either e-mail or fax. A reminder was sent after two weeks to those organisations that had not responded to the letter.

The collected privacy policies as well as privacy concerns of organisations were analysed by the researcher by counting the word from each criterion on National Principles.

Summary of Procedure

The following list summarises the procedure of this research.

Date	Procedure
24 August 1998 – 27 August 1998	□ Collect the List of the Top 100 Organisations from BRW magazine (Available at URL: http://www.brw.com.au); and □ Enter the demographic data into the observation checklist.
27 August 1998 – 12 September 1998	□ Search organisations on the Australian Yellow Pages (Available at URL: http://www.yellowpages.com.au); □ Fill up the observation checklist; and □ Send an e-mail to Information Collectors and Traders.
3 October 1998 – 17 October 1998	□ Search organisations on Web Crawler (Available at URL: http://webcrawler.com); □ Fill up the observation checklist; □ Send an e-mail to Information Collectors and Traders; and □ Send a reminder.
17 October 1998	□ Search organisations by entering the assumed addresses: ➢ 'http://www.(company name).com.au.'; and ➢ 'http://www.(company name).net.au'.
19 October 1998 –	□ Send a reminder; □ Enter the collected data in the observation checklist to SPSS; and □ Analyse and evaluate the collected privacy policies and their privacy concerns using the benchmark, 'National Principles for Handling Personal Information'. □ Produce the list of categorised concerns with its frequency count.

CHAPTER FOUR

RESULT/DISCUSSION

This chapter firstly describes the demographic data of sample used in this study. Secondly, each research question is answered and discussed from the findings obtained from this research. The findings must be viewed within the limitations of this study. Thus, the last section describes the constraints of this study.

Demographic Data of the Sample

All sample organisations were found to be large businesses (twenty or more employees). There were 42,700 businesses estimated in the total population (see Table 3.2). The demographic data comprises the industry distribution and the distribution of each sample organisations by state.

The industry distribution of the sample organisations is firstly divided into two categories: 'goods producing industries' and 'service industries'. (There was no sample organisation found in "agriculture, forestry and fishing industries".) Over the whole sample, the majority was in 'service industries' (69%) category and about one third (32%) was in 'goods producing industries'.

The industry distribution of the sample organisations in 'service industries' is shown in Table 4.1. (The number of businesses classified into accommodation, restaurant, cafẻ, and education industries were excluded from the population of 'service industries' in this table as no sample organisations classified into these industries.) The most common service industry in the top 100 organisations was 'wholesale trade' (19.8%), and the next ranked industry was 'retail trade' (16.8%). Lower percentages were found in 'finance and investment' (8.0%), 'insurance' (6.0%), and 'property and business services' (6.0%). The rest of industries comprised smaller percentages (less than 4.0%). 'Wholesale trade', 'retail trade' and ‘property and business services’ industries were the top three industries in the number of businesses in Australia (there were more than 4400 large organisations in each industry).

The industry distribution of the sample almost matched its distribution of the total businesses in ‘service industry’. As an exception, ‘finance and investment’ and ‘insurance’ made up of 3.8% of the total businesses, but a higher proportion of the sample organisations 13.8% (7.9% of ‘finance and investment’ and 5.9% of ‘insurance’) was included in this study.

Table 4.1: Distribution of Population and Sample in ‘Services Industry’

Services Industries	Number of Companies in Population	Proportion of Companies in Population	Number of Sample	Proportion of Sample
10. Whole sale trade	4,400	18.7%	20	19.8%
11. Retail trade	4,500	19.2%	17	16.7%
12. Transport and storage	1,200	5.1%	4	4.0%
13. Finance and investment	900	3.8%	8	7.9%
14. Insurance			6	5.9%
15. Property and business services	4,400	18.7%	6	5.9%
16. Health, community services	3,500	14.9%	3	3.0%
17. Personal, other services	700	3.0%	03	3.0%
18. Cultural, recreational services	900	3.8%	2	2.0%
Total	20,500	87.2%	69	68.2%

□ *Excluding accommodation, restaurant, café and education industry.*

Similarly, the industry distribution of the sample organisations in ‘goods producing industry’ is shown in Table 4.2. (The number of businesses classified into mining was excluded from the population of ‘goods producing industry’ as no sample organisations classified into these industries.) By comparison with the industry distribution of population in 'goods producing industry' (12.8%), there was a higher proportion of the sample organisations in this industry (31.8%) included in this study.

Table 4.2: Distribution of Population and Sample in Goods Producing Industry

Goods Producing Industries	Number of Companies in Population	Proportion of Companies in Population	Number of Sample	Proportion of Sample
1.Manufacturing: food	1,300	5.5%	12	11.9%
2.Manufacturing: machinery and equipment			3	3.0%
3.Manufacturing: printing and publishing			2	2.0%
4.Manufacturing: textiles and clothing			2	2.0%
5.Manufacturing: building materials			2	2.0%
6.Manufacturing: petroleum, chemicals, coal			1	1.0%
7. Manufacturing: metals products			1	1.0%
8. Manufacturing: wood and paper			1	1.0%
9. Construction	1,700	7.3%	8	7.9%
Total	3,000	12.8%	32	31.8%

□ *Excluding mining industry.*

Of all sample in 'goods producing industry', 'food manufacturer' was the most common industry (11.0%) followed by 'construction' (8.0%). Small percentages were found in the rest of 'manufacturers' in various products (less than 3.0%). Because there were only 1300 of the total large organisations classified in 'manufacturing', the total number of the sample organisations in 'manufacturing' (twenty-four organisations) included in this study was considerably large.

Table 4.3: Distribution of Population and Sample (by State)

State	Number of Companies In Population	Proportion of Companies in Population	Number of Sample	Proportion of Sample
New South Wales	9,400	31.5%	43	42.5%
Victoria	8,400	28.2%	30	29.7%
Queensland	4,900	16.4%	10	9.9%
South Australia	3,100	10.4%	5	5.0%
Western Australia	2,200	7.4%	13	12.9%
Tasmania	800	2.7%	0	0.0%
Australian Capital Territory	500	1.8%	0	0.0%
Northern Territory	500	1.8%	0	0.0%
Total	29,800	100.0%	101	100.0%

❑ *Including the number of large private sector businesses both in goods producing and service industries.*

The distribution of the sample organisations by state is shown in Table 4.3. The locations of the top 100 organisations were in various states in Australia but there was no sample organisation found in Tasmania, Northern Territories and Australian Capital Territory. Of the top 100 organisations, the highest percentage was located in New South Wales (42.5%). The second most common location of the sample organisation was Victoria (29.7%). Although the distribution of organisations in Victoria (28.2%) almost matched its population, there was a little higher percentage of the sample taken from New South Wales comparing to its population (31.5%). Similarly, Western Australian organisations occupied 12.9% of the top 100 organisations although the population of large organisations located in Western Australia was relatively a small proportion (7.4%). On the other hand, the sample organisations in Queensland occupied 9.9%, and a small percentage (5.0%)

of organisations was located in South Australia, although a higher proportion of the population was located in Queensland (16.4%) and South Australia (10.4%). The industry distribution and the distribution of states in the sample organisations were taken into consideration before drawing the answers from the findings of this study. The following sections describe the findings of this research, and conclude the answers of each question.

Business Activities on the Internet

In this section, the first question of this research is answered:

> *"Are Australian organisations participating in the Internet, if so, to what extent do they use it?"*

In identifying their use of the Internet, the sample organisations were allocated into six categories using the classification developed in the earlier section. The proportion of the sample organisations fallen into each category is shown in Figure 4.1.

Figure 4.1: Business Activities on the Internet

In the following section, their actual business activities of the sample organisations in each category are described. It describes the industry distribution (see Table 4.4 and Table 4.5) and the distribution of the sample by state (see Table

4.6) as to identify the trends of each industry and each state. At the end of this section, the answer to question one is summarised.

Non Internet Users

While the business use of the Internet was found to be very popular among Australian organisations, there were still a smaller number of sample organisations (27.7%) that were not using it. As described in earlier section, searches by the company (name using two most commonly used search engines) were attempted. Furthermore, assumed web site addresses; http://www.(companyname).com.au or http://www.(companyname).net.au, were entered into URL as an attempt of finding them. Those organisations that could not be found in this search process were assumed to be not connected to the Internet backbone and/or they do not publish their site on the Internet.

Of all Non Internet users (28), the larger number of organisations (17) in 'services industry' were found in this category compared with the number of organisations in 'goods producing industry' (11). However, seventeen organisations in 'service industry' represented only 24.6% in this industry. On the other hand, eleven organisations in the 'goods producing industry' were equivalent to 34.3%. Therefore, it indicated that more organisations in 'goods producing industry' did not use the Internet than those in 'services industry'.

Table 4.4: Business Use of the Internet (by Industry)

	Goods Producing Industry		Service Industry		Number of Companies	
1. Non Internet User	11	34.3%	17	24.6%	28	27.7%
2. Information Provider	16	50.0%	25	36.2%	41	40.6%
3. Information Collector	2	6.3%	16	23.2%	18	17.8%
4. Trader	0	0.0%	7	10.1%	7	6.9%
5. Restricted Trader	1	3.1%	1	1.5%	2	2.0%
6. Under Construction	2	6.3%	3	4.4%	5	5.0%
	32	100.0%	69	100.0%	101	100.0%

Table 4.5: Business Use of the Internet (by industry in details)

Industry	Non Internet User	Information Providers	Information Collectors	On Line Traders	Restricted Traders	Under Constructors	Total
Goods Producing Industry							
1. Manufacturing: food	5	5	1	0	1	0	12
2. Manufacturing: machinery and equipment	1	2	0	0	0	0	3
3. Manufacturing: printing and publishing	1	0	0	0	0	1	2
4. Manufacturing: textiles and clothing	0	1	1	0	0	0	2
5. Manufacturing: building materials	0	2	0	0	0	0	2
6. Manufacturing: petroleum, chemicals and coal	0	1	0	0	0	0	1
7. Manufacturing: metals products	0	0	0	0	0	1	1
8. Manufacturing: wood and paper	0	1	0	0	0	0	1
9. Construction	4	4	0	0	0	0	8
	11	16	2	0	1	2	32
Services Industry							
10. Whole sale trade	7	5	4	2	1	1	20
11. Retail trade	4	10	2	1	0	0	17
12. Transport and storage	1	1	1	0	0	1	4
13. Finance and investment	2	1	3	2	0	0	8
14. Insurance	1	2	3	0	0	0	6
15. Property and business services	0	4	1	0	0	1	6
16. Health, community services	1	2	0	0	0	0	3
17. Personal, other services	0	0	2	1	0	0	3
18. Cultural, recreational services	1	0	0	1	0	0	2
	17	25	16	7	1	3	69
	28	41	18	7	2	5	101

Table 4.6: Business Use of the Internet (by State)

	NSW		VIC		QLD		SA		WA	
		%		%		%		%		%
1. Non Internet User	12	27.9	6	20.0	4	40.0	1	20.0	5	38.5
2. Information Provider	16	37.2	12	40.0	4	40.0	3	60.0	6	46.1
3. Information Collector	10	23.3	6	20.0	1	10.0	1	20.0	0	0.0
4. Trader	2	4.6	4	13.3	0	0.0	0	0.0	1	7.7
5. Restricted Trader	0	0	0	0.0	1	10.0	0	0.0	1	7.7
6. Under Construction	3	7.0	2	6.7	0	0.0	0	0.0	0	0.0
	43	100	30	100	10	100	5	100	13	100

By analysing the distribution of the sample by state, the least use of the Internet was found in Queensland (40.0%) followed by Western Australia (38.5%). New South Wales (27.9%) came third in this category and lower percentages were found in Victoria (20.0%) and South Australia (20.0%). This indicated that the remote states: Western Australia and Queensland, appeared to be slower in having an Internet presence.

Information Providers

In this study, the majority of the sample was found to be Information Providers (40.6%). Those organisations used the Internet mainly for advertising and recruiting purposes. Although they often provided a feedback form, regarding their Web site and/or services and products, to fill in, they did not collect personal details that the company could identify and contact a person in a real world. They could only identify a person on the Internet by an e-mail address and use it for contacting the person. Some organisations provided subscription services through e-mail facilities to keep their existing and/or potential customers inform of their products and/or services.

Half of the sample organisations in 'goods producing industry' (50.0%) and a smaller proportion (36.2%) in 'service industry' were classified as Information

Providers. These proportions showed that Information Providers were the most prevalent form of business in both of industries.

The majority of the sample organisations in each state were fallen into the Information Provider category. However, New South Wales showed the lowest percentage as Information Providers (37.2%). In fact, more organisations in New South Wales were forming other types of business on the Internet, which are described in the following sections.

Information Collectors

Information Collectors were the next ranked form of business on the Internet. (17.8%) These sites contained two types of forms in general: feedback forms and/or application forms.

A typical feedback form used by Information Collectors gathered users' impression on their Web site, products and services. However, they collected personal information including addresses, telephone numbers so the company could contact users in a real world. A typical application form provided on the Internet required almost all details necessary to fill out a normal application form required in a real world. The only difference was that the application form filled out on the Web site would be sent to the person by mails for its completion along with an invoice statement. The method of payment was not normally mentioned on the Web site. In fact, they used conventional methods such as in-person, cheque, money order, and bank account or credit card by mail, fax, or phone.

A very small proportion of the sample organisations in 'goods producing industry' was acting as Information collectors (6.3%) while a much larger proportion in service industry (23.2%) used the Internet for this purpose. It seems that the organisations in 'service industry' were more interested in personal information than that of the goods producing sector.

Organisations in New South Wales showed the highest percentage of Information Collectors (23.3%). The next ranked states were Victoria (20.0%) and South Australia (20.0%). Queensland showed a smaller percentage in this form (10.0%) and no Western Australian organisations were found to be Information Collectors.

On-line Traders

Only a small percentage of the sample organisations were found to be on-line traders (6.9%). They allowed customers to order products/services and also to pay on the Internet by providing credit card information. Interestingly, most organisations offered their customers an option of sending credit card information using conventional methods (by mail, fax, or telephone). For those do not have credit cards or do not like to use credit cards, organisations offered other payment options such as follows:

1. By direct debits from Australian bank accounts;
2. By cheques restricted to Australian currency;
3. Via wire transfer for users in overseas.

One of the reasons for the company providing these options was "for those customers who do not understand and do not trust the secure credit card transaction methods the company provides." (an Internet Administrator, personal contact, 1999). "Although a small portion of total sales (approximately 10.0%) was conducted using conventional methods, the majority of users (approximately 90.0%) normally chose to send Credit Card information on the Internet." (a System Administrator, personal contact, 1999). A recent survey of Internet users also found that 75% of the survey participants are willing to use Credit Cards on the Internet. (GVU's Tenth WWW User Survey, 1998).

The study found that none of the goods producing industry was using the Internet for trading purposes. Although a small proportion of the sample (10.1%) has fallen into this category, all traders were in the 'service industry'.

On-line trade was most common in Victorian based organisations; 13.3% of the sample in Victoria was found to be On-line Traders, followed by those in New South Wales (4.6%). One organisation in Western Australia was found to be an on-line Trader. No organisation in the other states used the Internet for on-line trading purposes.

Restricted Traders

Only a small number of organisations (2.0%) were classified into this category. These organisations had their Web site address on the Internet where the Internet users could easily access. However, they only allowed people within the organisation and their trading organisations to view their sites. These organisations often required a special browser to view their site. Therefore, the access was forbidden as soon as the server detected an unmatched browser that commonly used by many of the Internet users such as the Internet Explorer and the Netscape Navigator.

The results showed that the use of the Internet for this purpose appeared in both 'goods producing industry' and 'service industry' and two restricted traders were located in Queensland and Western Australia.

Under Construction

Beside those organisations that already operated the business on the Internet, there were a small percentage of organisations (5.0%) that reserved a site for future development. Their Web sites often contained a simple message such as 'Under Construction'. There was no other information regarding a completion date or its use. Therefore, the future study has to be conducted in order to investigate their use of the Internet. Those organisations were found in both 'goods producing industry' and 'service industry', and it appeared that more organisations in New South Wales and Victoria were considering the use of the Internet.

Trends in the Use of the Internet (Summary of Question 1)

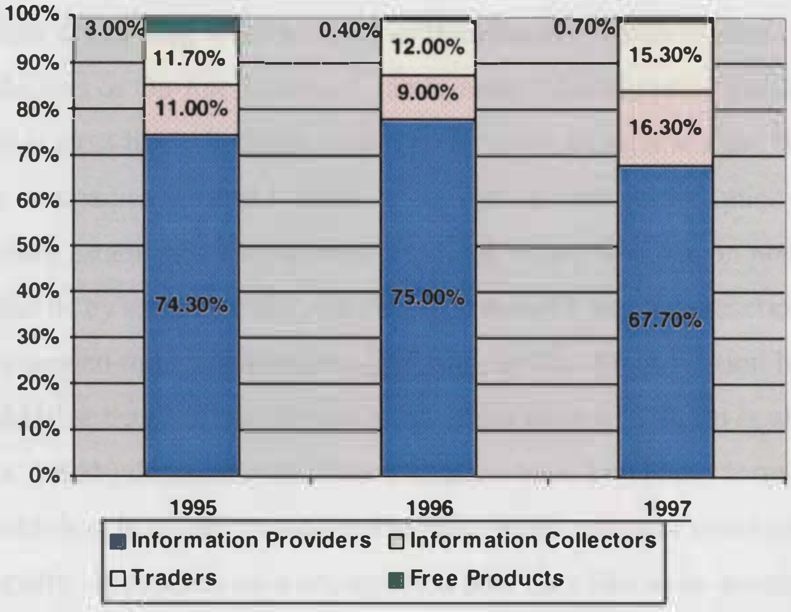
The business use of the Internet was found to be prevalent among Australian large private sector organisations. In fact, the result of this research showed that the majority (72.3%) of the Australian organisations was using the Internet for business purposes. Further, more organisations (5.0%) were reserving their site for the future use at the time of data collection period between 28 August 1998 and 17 October 1998.

The most common form of business on the Internet was the Information Providers. This result reflected a continuous study (Ng et al., 1998) that investigated into universal organisations in various industries selected from 'Yahoo! Directory' on the business use of the Internet. It also reported that the majority had a web presence for providing basic information (see Figure 4.2).

When presenting the study of Ng et al. (1998), a modification was made to its classification. That is, the following classifications in their study are presented as Information Providers in Figure 4.2:

- ❑ Basic web presence – a web presence with basic information about the company but no further details on specific products on services;
- ❑ Provide information – a web presence with company information and some information about products or services;
- ❑ Price information – a web presence with company information and products or services information together with some price details but with facilities for conventional purchasing only.

Figure 4.2: Change in Use of Web sites
(Modified Ng et al., 1998)



Similarly, the following classifications in their study was presented as Information Collectors in Figure 4.2:

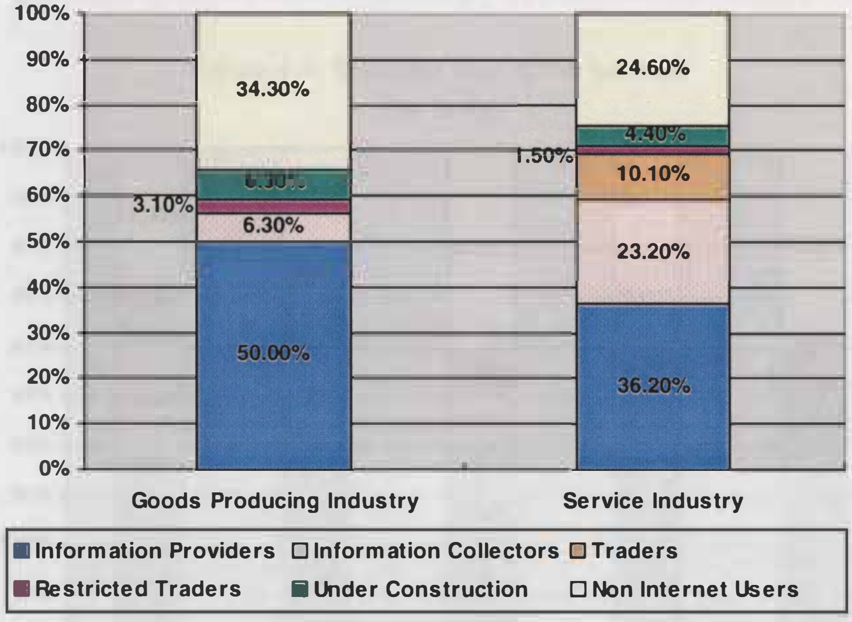
- ❑ E-mail Ordering – a web presence with company information and products or services information together with some price details and the ability to order products or services via electronic mail but with billing occurring conventionally;

- ❑ Registration of Credit Card Details – a web presence with company information and products or services information including price details with pre-registration of credit card details by conventional means to gain account number which may be used to order goods on-line.

Between 1995 and 1996, Information Providers showed a slightly increased proportion of75.0%. However, it decreased by 4.0% between 1996 and 1997. On the other hand, these continuous reports showed that the proportion of On-line Traders had been slowly increasing in the last three years. "Almost all firms were very interested in the Internet and almost all of the companies have plans to increase the ways and the extent to which they use the Internet as a vehicle for EC to fully tap its potential and benefits" (Nath et al., 1998, p.96). So the result of Ng et al. (1998) probably indicated that many organisations in the world were gradually moving from simple Information Providers to Information Collectors or Traders.

However, this study showed that Information Providers were the most common form of business in Australia. "A number of clients' contacts/requests increases when the Web site does not require any specific personal information. Thus, organisations are finding it better to act as Information Providers than Information Collectors or On-line Traders." (an Internet Administrator, personal contact, 1999) It is most likely because people prefer to be anonymous and they are happy to contact companies through e-mails only. The Internet permits anonymity, however, anonymity establishes the potential for fraud, either by a person pretending to be someone else or by some one denying that they entered into a transaction which has subsequently proved to be inconvenient (Pattison, 1997). Identification is important to build trust between two parties on a certain matter. Shapiro et al. (cited in Ratnasingham, 1998b) describes that, "Identification-base Trust" is a form of trust that is easily established in an electronic environment where partners never meet each other physically. It depends on a organisation how they like to be involved in the Internet, and also it depends on what they sell. In fact, this study also indicated that the use of the Internet closely relates to the type of industry the organisation is in (see Figure 4.3). That is, goods producing industries are using it mainly for providing information while some services industries are proactively using it for collecting information on the Internet.

Figure 4.3: Business Use of the Internet
(by Industry)

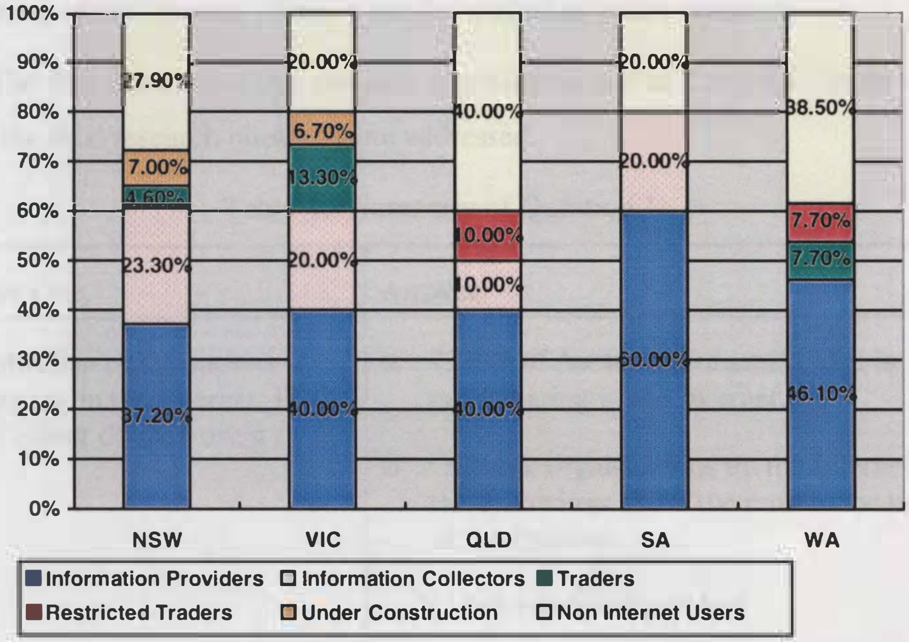


"Only certain types of products sell better over the Web than others." (Angelides, 1997, p.413) The Internet provides more opportunities for the industries dealing with these products and services that can be investigated, purchased and delivered over the Internet (Ng et al., 1998). Angelides (1997) describes the examples of leading web products and services such as computers and accessories, software, travel services, insurance, and financial services. Many of the service industries, in fact, offer intangible products that can not only be advertised but also sold and distributed on the Internet. Therefore, more service industries could take the full advantages of the Internet than those in 'goods producing industry'.

Also, some differences in the use of the Internet were observed by states (see Figure 4.4). Firstly, the use of the Internet was found to be similar between New South Wales and Victoria. Although the proportion of each category differed between the two states, the sample organisations in both of these states were participating on the Internet proactively. That is, New South Wales and Victoria states were using the Internet for providing and gathering information as well as trading purposes.

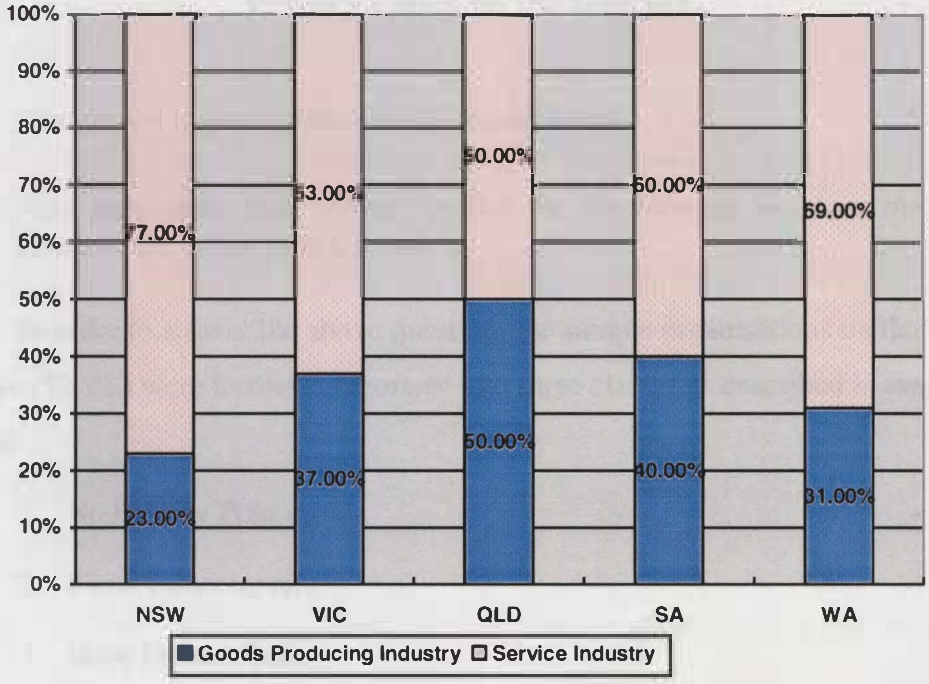
Secondly, Queensland and Western Australia were found to have the least number of organisations using the Internet, and this study found that only the organisations in those two states were found to be Restricted Traders. It was an interesting result that they were not appeared in the earlier use of the Internet, because Queensland and Western Australia are the most remote states in Australia.

Figure 4.4: Business Use of the Internet
(by State)



Finally, the majority of the sample organisations in South Australia were found to be on the Internet, though they generally acted as Information Providers and Information Collectors only.

Figure 4.5: Industry Distribution by State



The reason of the differences in the use of the Internet by states was not because more goods producing industries were studied in both Queensland and Western Australia (see Figure 4.5). The reason could not be found in this study because this study did not study organisational decisions making process in involvement of the Internet. Thus, it can be studied in future research.

The first question of this research was summarised in Table 4.7. In the next section, the final research questions are addressed.

Table 4.7 Summary of Question 1

Question One	Answer
Are Australian organisations participating in the Internet, if so, to what extent do they use it?	□ 72.3% of Australian organisations is participating in the Internet. □ Of those organisations on the Internet, the followings show the rank in the use of the Internet: ➢ Information Providers ➢ Information Collectors ➢ On-line Traders ➢ Restricted Traders

Privacy Policy on the Internet

The second major question in this research was,

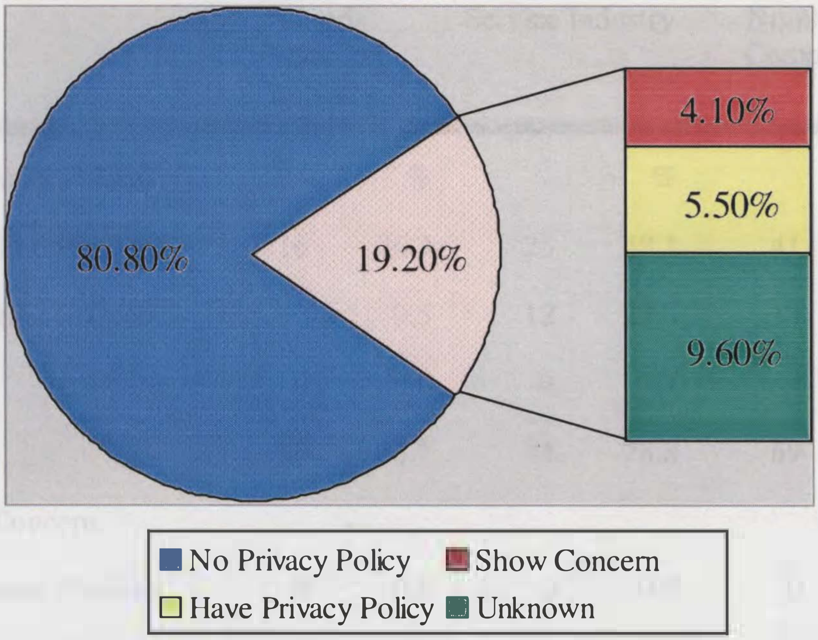
"Do they show their privacy policy on the Internet or show the concerns on privacy protections?"

In order to answer the above question, the sample organisations on the Internet (72.3%) were further categorised into three classes as described in the earlier section:

1. No Privacy Policy;
2. Show Concern; and
3. Have Privacy Policy.

The proportion of the sample organisations fallen into each category was shown in Figure 4.6.

Figure 4.6: Privacy on the Internet



Due to the inaccessibility of both the sites of ‘restricted traders’ and ‘under construction’ (9.6%), this study was unable to determine whether they publish their privacy policy on the Internet. Therefore, only the sample organisations in the Information Provider, Information Collector and On-line Trader categories were examined in this section.

The following tables show the frequency of the sample organisations in each category by industry (see Table 4.8) and by state (see Table 4.9). In the following section, each category was analysed in terms of their business activities on the Internet as well as the distribution of states and industries. Privacy policies as well as privacy concerns both published and unpublished were analysed using the benchmark described in the earlier section. At the end of this section, current trends in privacy issues were summarised as the answers to the question two and three.

No Privacy Policy

A high proportion of the sample organisations with Web sites fall into this category (80.8%). These organisations did not have a privacy policy and also did not have any statement on privacy issues or handling of personal information on the Internet.

Table 4.8: Privacy Policy on the Internet (by industry)

	Goods Producing Industry		Service Industry		Number of Companies	
1. No Privacy Policy		%		%		%
- Information Provider	16	76.2	25	48.1	41	56.1
- Information Collector	2	9.5	12	23.0	14	19.2
- Trader	0	0.0	4	7.7	4	5.5
	18	**85.7**	**41**	**78.8**	**59**	**80.8**
2. Show Concern						
- Information Provider	0	0.0	0	0.0	0	0.0
- Information Collector	0	0.0	0	0.0	0	0.0
- Trader	0	0.0	3	5.8	3	4.1
	0	**0.0**	**3**	**5.8**	**3**	**4.1**
3. Have Privacy Policy						
- Information Provider	0	0.0	0	0.0	0	0.0
- Information Collector	0	0.0	4	7.7	4	5.5
- Trader	0	0.0	0	0.0	0	0.0
	0	**0.0**	**4**	**7.7**	**4**	**5.5**
4. Unknown						
- Restricted Trader	1	4.8	1	1.9	2	2.7
- Under Construction	2	9.5	3	5.8	5	6.9
	3	**14.3**	**4**	**7.7**	**7**	**9.6**
	21	**100.0**	**52**	**100.0**	**73**	**100.0**

Table 4.9: Privacy Policy on the Internet (by State)

	NSW		VIC		QLD		SA		WA	
		%		%		%		%		%
1. No Privacy Policy										
- Information Provider	16	51.6	12	50.0	4	66.6	3	75.0	6	75.0
- Information Collector	8	25.8	4	16.8	1	16.7	1	25.0	0	0.0
- Trader	2	6.5	2	8.3	0	0.0	0	0.0	0	0.0
	26	**83.9**	**18**	**75.1**	**5**	**83.3**	**4**	**100**	**6**	**75.0**
2.. Show Concern										
- Information Provider	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
- Information Collector	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
- Trader	0	0.0	2	8.3	0	0.0	0	0.0	1	12.5
	0	**0.0**	**2**	**8.3**	**0**	**0.0**	**0**	**0.0**	**1**	**12.5**
3. Have Privacy Policy										
- Information Provider	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
- Information Collector	2	6.4	2	8.3	0	0.0	0	0.0	0	0.0
- Trader	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
	2	**6.4**	**2**	**8.3**	**0**	**0.0**	**0**	**0.0**	**0**	**0.0**
4. Unknown										
- Restricted Trader	0	0.0	0	0.0	1	16.7	0	0.0	1	12.5
- Under Construction	3	9.7	2	8.3	0	0.0	0	0.0	0	0.0
	3	**9.7**	**2**	**8.3**	**1**	**16.7**	**0**	**0.0**	**1**	**12.5**
	31	**100**	**24**	**100**	**6**	**100**	**4**	**100**	**8**	**100**

The result showed that no organisation in the goods producing industry published their privacy concerns on the Internet. Moreover, the majority of the sample organisations in the service industry showed no privacy concerns on the Internet (78.8%). The result of this study showed that the largest number of organisations in this category were Information Providers (56.1%), however, there were also Information Collectors (19.2%) and On-line Traders (5.5%) fallen into this category. As the Web sites developed by Information Providers published information only and they did not intend to collect personal information on the Internet. Therefore, it is understandable that they find no necessity of publishing privacy concerns on the Internet. However, Information Collectors and On-line Traders' Web sites intended to collect personal information that could be useful for marketing purposes. Therefore, some concern for privacy is desirable. By further analysing Information Collectors and On-line Traders that showed no privacy concerns, it showed that those organisations were in the following industries; 'wholesale trade' (6), 'retail trade' (4), 'finance and investment' (2), 'insurance' (2), 'property and business services' (1), and 'transport and storage' (1). The information they collect was not only of a nature that could identify the person but also the information that indicated clients' financial, health and other situations/conditions. Moreover, the information they collect was often not even relevant for their product/service provided.

Instead of publishing privacy concerns, these Web sites often showed the statements on their legal liability. The 'legal issues' and 'disclaimer' sections contained the issues such as below:

- ❑ The data and information ("Information") on this site is provided solely for general illustration and instructional purposes and is not intended to address any circumstances of any particular individual or entity;
- ❑ The site may be linked to servers or web sites maintained by other organisations. The company cannot provide any warranty about the accuracy or source of any data set out on any of those servers or Web sites or the content of any file the user downloads from such a third party site;
- ❑ The company does not represent or warrant that any files obtained from or through this site are free from computer viruses or other defects. The user must assume all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of those files and the company's liability in such an event is limited to the re-supply of those files; and

- ❑ All trademarks mentioned on this site belong to the respective owners. The company owns the copyright in all Information contained in this site. Users may reproduce the Information in whole or in part provided it is not intended for public or commercial purposes and any notices of attribution or copyright are retained in the reproduced materials.

These items are frequently shown on the Internet by many organisations. It seems that legal liabilities are more of a concern among Australian organisations at this time.

The locations of the sample organisations were in various states. As the majority of the sample organisations in each state showed no concerns (over 75.0%), those organisations fallen into other categories were further analysed in the following sections.

Show Concern

There was a very small proportion of organisation showed their concerns on privacy issues (4.1%). The information collected on privacy concerns shown on the Internet was analysed, and the most popular privacy implementation methods that were stated on the Internet are shown in Table 4.10.

Table 4.10: Privacy Concern Shown on the Internet

Privacy Protection	Number of Companies
SSL Technology to help protect the Information	3
128 – bit encryption of all communication	2
User authentication	2
Encryption of Stored Data	2
Tamper proof data transmission	1
Secure access to Servers	1

Interestingly, all organisations mentioned the use of SSL technology as a protection of the information sent over the Internet. As described in the earlier sections, SSL is an encryption method of protecting information that is normally supported by most popular browsers: the Internet Explorer, Netscape Communicator. This can protect personal information sent on the Internet by allowing only intended recipients to read information that is encrypted, but the question still remains how securely information are stored and how ethically the company use this information.

Other privacy protection mentioned were; 128–bit encryption of all communication, user authentication, encryption of stored data, secure access to servers and tamper proof data transmission. Most of those are described in the earlier sections. Cryptography is the main technological protection offered by those organisations. In fact, 128-bit encryption was often mentioned. 128-bit encryption is known as a strong encryption key. The longer bits make it difficult to crack it (Pompili, 1996). However, in December 1999, the Wassenaar Arrangement was signed by 33 governments around the world including Australia to ban strong cryptography such as 128-bit encryption (Davidson, 1999a; Davidson, 1999b). As encryption software is attractive to potential criminals and terrorists, many countries are wary of its use. This implies that technologies themselves do not fully protect privacy. Therefore, a privacy policy should ideally be published to notify Internet users on organisations' conduct (Agranoff, 1991; Bridis, 1999).

The organisations in this category were all found to be On-line Traders: two organisations in Victoria that were classified as 'cultural and recreational services', 'finance and investment', and one 'personal and other services' organisation in Western Australia. These were equivalent to nearly a half of all On-line Traders (42.9%) identified in this study. In fact, this study found that none of On-line Traders showed their privacy policy on the Internet. It indicated that On-line Traders were approaching privacy issues at the technological level while some were approaching it by publishing a privacy policy. In the next section, the organisations that published their privacy policy are discussed.

Have Privacy Policy

Privacy policies were found on the Internet occurred in only a small number of the sample (5.5%). All organisations in this category were found to be

Information Collectors. They consist of two 'wholesale trade' organisations in New South Wales and two organisations in Victoria that classified into 'personal and other services' and 'finance and investment'. Privacy policies were rather privacy statements, that is, a simple sentence saying how they protect customer's privacy. Of the four organisations that provided privacy statements, surprisingly, two organisations in New South Wales stated that,

> *"the information sent is protected by the use of SSL technologies, however, the privacy of information sent and received is not guaranteed."*

New South Wales was the state that was highly involved in the development of privacy protection law in Australia. In fact, both of the Privacy Commissioner and Australian Privacy Charter Council were located in this state. Although privacy was mentioned in the above statement, it was protected only by the capabilities of SSL technology.

On the other hand, an organisation in Victoria stated that;

> *"personal details are not passed outside the company's network."*

Another organisation in Victoria stated that;

> *"the company will take all reasonable steps to protect privacy and that the information is for the sole use of the company and its subsidiaries and will not be sold or released to any third party."*

These statements explained how they handled personal information collected on the Internet. However, they did not meet the requirement of 'National Principles for Handling of Personal Information'. In fact, out of ten National Principles, these statements only covered one principle: the Use and Disclosure of Personal Information (Table 4.11).

Smith et al. (1996) identified four dimensions of individuals' concerns about organisational information practice: Collection, Errors, Secondary Use and Improper Access. These four dimensions are also covered in 'National Principles for Handling Personal Information'. These are probably the minimum issues that should be covered by organisations as privacy protection. The organisations in Victoria presented the best privacy practice in Australia but these statements need to be improved much more in order to meet the National Principles. In the next section, unpublished privacy policies are presented to discuss the matter in details before summarising the answers to Question two and Question three,

Table 4.11: Privacy Policy Shown on the Internet

National Principles for Fair Handling of Personal Information	Number of Companies Mentioned
Collection	0
Use and Disclosure	2
Data Quality	0
Data Security	0
Openness	0
Access and Correction	0
Identifiers	0
Anonymity	0
Trans-border Data Flows	0
Sensitive Information	0

Unpublished Privacy Policy

The letter requesting their corporate privacy policy was sent to Information Collectors and On-line traders found in this study. After sending follow-up letters, 36.0% of them responded. Cooper and Emory (1995, p.282) stated "a return rate of bout 30 percent are often considered satisfactory." On the other hand, Erdos (cited in Zikmund, 1991, p.175) stated "no mail survey can be considered reliable unless it has a minimum of 50.0% response, or unless it demonstrates with some form of verification that the non-respondents are similar to the respondents." As the requesting letter only encouraged those that had a privacy policy to reply, it was most likely that non-respondents did not have a privacy policy or unaware of such policies. However, it could not be assumed that they did not have a privacy policy. Therefore, this study separated 'No Response' from 'no Privacy Policy'. No further investigation was conducted to increase the response rate, thus, the findings might not be considered reliable according to Erdos.

Out of all respondents (36.0%), over a half of them (20.0 %) answered that they have no privacy policy at all (see Table 4.12). Some (8.0%) answered that they do have a privacy policy but also have a policy not to reveal the privacy policy to the public. The rest (8.0 %) answered that they have a privacy policy but it is currently under revision. As a result, no organisation had a completed privacy policy that could be published on the Internet.

In the following section, the replies of these respondents were analysed, and the given comments are presented.

Table 4.12: Unpublished Privacy Policy

Results	Information Collector		On-line Trader		Total	
		%		%		%
Have Privacy Policy but have a policy not revealing such policies to Public	2	11.0	0	0.0	2	8.0
Have Privacy Policy but now under revision stage	2	11.0	0	0.0	2	8.0
No Privacy Policy exist	2	11.0	3	42.9	5	20.0
No Response	12	67.0	4	57.1	16	64.0
	18	100.0	7	100.0	25	100.0

Privacy Policy with Non-Releasing Policy

The two organisations that had their corporate privacy policy but also had a policy not revealing such policies were both Information Collectors in New South Wales: 'insurance' and 'property and business services'. One of these organisations informed that they also had 'Internet Policy' that was released to all employees who use the Internet. According to the representative of this organisation, an Internet Policy was a strict policy on use of e-mail and the Internet. This policy was also supported with strict penalties. For example, a misuse of e-mail and/or the Internet may result in termination of their position. It indicated that organisations that were aware of this matter establish more than one policy to protect information.

On the other hand, the other organisation that answered they have the privacy policy stated that,

> *"Our corporate privacy policy is developed using the benchmark, 'National Principles for Fair Handling of Personal Information', established by the Privacy Commissioner in 1998."*

This means that their privacy policy covered National Principles, though the existence of a non-releasing policy stops people from accessing it.

The fifth principle, 'Openness', states that,

> *"An organisations should have clearly expressed policies on its management of personal information which should be readily available."*

Furthermore, in guidance notes to principles of this section, it was stated that,

> *"A written policy would probably be a sensible step, though this principles does not require it as such."*

This statement was unchanged in the revised edition of National Principles for the Fair Handling of Personal Information released in January 1999. According to this current benchmark, the organisations with a non-releasing policy still met its requirement.

Privacy Policy under Revision

The organisations at the revision stage of privacy policy were also Information Collectors in NSW and Victoria. They were in 'transport and storage' and 'personal and other services' industries. Although they were aware of problems in current privacy policy, one of these organisations provided their current privacy policy for this study. Their current privacy policy was evaluated using the benchmark. The result of its evaluation was shown in Table 4.13.

Table 4.13: Quality of Unpublished Privacy Policy

National Principles for Fair Handling of Personal Information	Coverage
Collection	0
Use and Disclosure	1
Data Quality	1
Data Security	0
Openness	0
Access and Correction	1
Identifiers	0
Anonymity	0
Trans-border Data Flows	0
Sensitive Information	0

After the evaluation, it was found that their current privacy policy did not completely meet the requirements of National Principles. The policy covers 'use and disclosure', 'data quality', and 'access and correction' principles. However, the representative of this organisation informed that,

> *"the privacy policy is in the process of revision in order to meet the National Principles, and the release of the new policy is subject to Australian government's requirement."*

When the government introduces a new regulation that obliges organisations to provide a privacy policy, the company will introduce them to the public. This comment emphasises the importance of the government's role in facilitating privacy issues.

No Privacy Policy

Out of all organisations (20.0%) that had no corporate privacy policy, some of them were On-line Traders in Victoria. The others were Information Collectors also located in Victoria. Most of them were in 'finance and investment' industry, and the rest were in 'cultural, recreational services' and in 'manufacturing'. Most organisations had no corporate privacy policy because they considered that they were not collecting personal information. They considered that they had a basic Web site, therefore, there was no need to establish a privacy policy. Also, they believe that the technologies in use protect clients' privacy, and deemed to be sufficient. The privacy protection concerns provided by respondents were listed in Table 4.14.

Table 4.14: Current Privacy Protection

Privacy Protection	Number of Respondents
A few authorised employees have access	3
Firewall on LAN	2
ISDN line between government	1
'Code of Conduct' covers dealings of personal information	1
Encryption of stored data	1
Automatic virus checking of incoming Internet materials	1

The most popular privacy protection concern provided by respondents was that only a few authorised parties had access to databases that collected and stored personal information. Normally, only a couple of people within organisations have access to stored information using password facilities. Secondly, they stated that the use of firewalls on LAN protected data from unauthorised parties. Firewalls were mentioned in the previous section, and it had become apparent that they were not sufficient in privacy protection.

Furthermore, an organisation mentioned the use of ISDN (Integrated Services Digital Network) line to send information to Government. The Internet can be connected either by connecting to the Internet backbone directly or thorough an ISP (Internet Service Provider) who connects to the Internet backbone. Currently, the link to them is over a standard telephone, or ISDN. "ISDN is a dial-up digital link that offers high-speed and virtually error-free data transmissions." (Collin, 1997, p.17) Thus, it is claimed to provide data integrity, which it does not.

Some organisations had policies to control the conduct of employees. For example, 'Code of Conduct' covers the use of information. The part of code was provided as stated as below:

> *"Directors and employees shall not use confidential and/or official Authority information to gain improper advantage for themselves or for any other person or body, in ways which are inconsistent with the obligation to act impartially, or to improperly cause harm or detriment to any person, body or the Authority."*

However, this is a generic code that is not established specifically for Internet dealings. Codes of Ethics do have an effect on some computer abuse judgements and intentions, moreover, Information Systems specific codes have a direct effect on sabotage judgements and intentions (Harrington, 1996). Thus, it will be appropriate to develop a policy specifically for Internet dealings.

Finally, organisations were approaching this issue under some assumptions. For example,

> *"it is assumed that staff are aware of the security risks associated with using e-mail and do not use this for transfer of sensitive/confidential information." (a Information Systems Manager, personal contact, 1999).*

It seems that most organisations without policies rely on the capabilities of existing technologies and/or they believe in ethical conduct of authorised people by providing a code of ethic.

In the next section, the findings of this research are summarised to answer the question two and three.

Trends in Privacy Protection (Summary of Question Two and Three)

As a result of this study, it clearly indicates that there is a lack of privacy concern by Australian organisations although the Internet is commonly used by Australian organisations. It reflects to the parallel study of corporate privacy policy in Australia by Brooks (1999), an Australian Business Consultant. His study also concluded that only 5% of the 79 companies that have a web site in the top 100 Australian organisations based on market capitalisation have an online privacy policy. Similarly, in the survey of the 50 Australian Web sites most accessed by Australians, only 20.0% mention anything about the privacy of personal information. The result of this survey presents Australian corporate practices in April 1999, which is six months after this study was conducted. It implies that Australian privacy protection practices have not changed dramatically between October 1998 and April 1999.

On the other hand, a new survey of Web sites privacy policies in the United States of America has found dramatic improvement (Kathleen, 1999). While a government study last year found that only 14.0% of sites published privacy policies, the Georgetown Internet Privacy Policy Study showed that 66.0% of the sample Web sites posted a privacy policy (Bridis, 1999). The American privacy practices seem to be much better. However, there is an argument of a need for a legal framework that gives a guidance to companies about what they should be doing, and provides an enforcement mechanism when self-regulation itself is not enough, said Grant, vice president of public policy for the National Consumers League (cited in Murphy, 1999b).

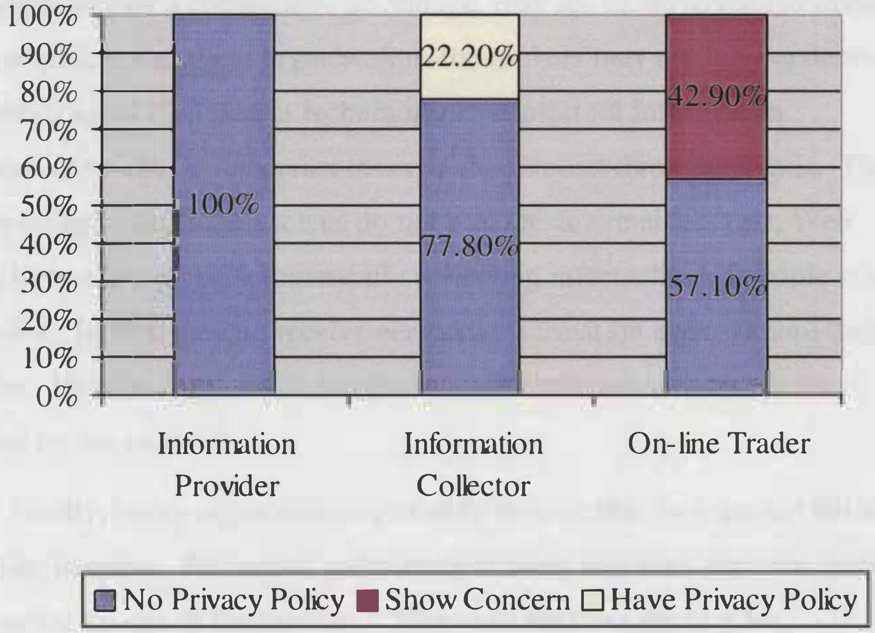
Lack of privacy policies does not imply that privacy is not protected at all in Australia. According to Brooks (1999), the lack of a privacy policy is more likely to be due to not seeing it as a priority rather than anything sinister. Lack of privacy policies may, in fact, imply that there are less problems of privacy in Australia so they are not threatened to act in this matter as quickly as other countries.

At last, the findings of this study, in conjunction with previous studies, indicated that the current privacy protection level relateed to two aspects: their current business use of the Internet and their current level of threats. The following sections explain these issues in detail.

Current Business Use of the Internet

This study showed a clear relationship between the use of the Internet and the privacy protection level as shown in Figure 4.7.

Figure 4.7 Privacy Concerns and Business Use of the Internet



Information Provider. This study indicated that all Information Providers showed no concerns on privacy issues. The findings of this study, in conjunction with previous studies, explain the various reasons, as to why Information Providers show no concern on privacy issues.

First of all, as described in the earlier section, when organisations do not consider that they are collecting sensitive information that may threaten the privacy of clients, they do not show concern about clients' privacy.

Many current Information Providers do not ask for personal information, and do not consider that they are collecting personal information. However, sensitivity of information varies among individuals. Therefore, there is still a chance of them exposing information without knowing that it is sensitive for a person. Any information should be private (Pompili, 1996). Information Providers probably believe that clients do not send their sensitive information on the Internet. However, the Internet is widespread in the world and used by many people regardless of their age, sex, and occupations, and the Internet users differ in the level of understanding in its capabilities. Therefore, organisations can not assume that all clients fully understand the risks of exposing individual privacy from using the Internet.

Secondly, organisations tend to believe that technologies do only what they intended to do (Nath et al., 1998). Furthermore, Nath et al. (1998) described that, because organisations are seeing the Internet simply as an opportunity to gain a competitive advantage, they are likely to rush to obtain a Web presence, therefore, organisations themselves may not fully understand the capabilities of the Internet technologies. Almost all Information Providers allow clients to contact them on the Internet through e-mails. That is, even though clients themselves do not provide an e-mail address, Web servers have a feature of automatically collecting information of people who accessed it. In fact, they do receive personal information even without their intention. How do they handle this personal information sent by clients or collected by the servers?

Finally, many organisations probably believe that they are not liable if something happens. Privacy of individuals is taken into consideration more than ever by the use of the Internet. "However, they are waiting for legislation specifics" (a Information Systems Manager, personal contact, 1999). Many articles on privacy issues are pressuring private sector organisations to establish a privacy policy. Is it ethical that organisations wait for government to act, knowing it will take a long time for its complete process?

Many Australian organisations currently fall into the Information Provider category. It seems that privacy policies on the Australian Web sites will not increase unless they start establish/publish it by acknowledging the above points.

Information Collectors. The study showed that privacy policies were more likely to be provided by Information Collectors, even though the majority (77.8%) had no apparent concern with privacy issues. The only difference between Information Providers and Information Collectors is that Information Collectors require clients' addresses and phone numbers upon queries. Organisations use the information to contact the person for the query.

As a result of this study, Privacy policies that appeared on the Internet covered only the disclosure of its use: the information will be only shared within the organisation and its affiliates. The study of Smith et al. (1996, p.167) concluded that, "the highest levels of privacy concern were associated with Improper Access and Unauthorised Secondary Use." Thus, the use and disclosure may be the most important privacy concern for many people. However, as listed in IPPs, a statement on the use and disclosure itself may not be sufficient to alleviate privacy concerns at the organisational level.

On-line Trader. The study showed that privacy concerns not privacy policies were only shown by On-line Traders, though a higher proportion (57.1%) did not mention a word of privacy. They provided explanations on how securely information is sent and kept by the use of technology. Some obviously saw technological protection as a high priority (see Table 4.8). Organisations probably believe that technologies provide the sufficient tool to protect the privacy of individuals. Furthermore, organisations are likely to see that clients are only concerned about the security aspect of on-line trading since their clients have to provide Credit Card information. However, the chance of information mistreated by employees does not decrease in the technologically secured space. It could be possible to state that organisations are likely to consider that their clients trust the conduct of the organisations. It could be acceptable within a certain culture, but they are potentially trading with people around the whole world on the Internet. Trading requires two parties: supplier and buyer. It is ideal that both parties are able to collect sufficient information on the Internet to build trust without seeing a person. Building trust between two parties could be the key issue to on-line trading.

The Current Level of Threats in Australia

Lack of privacy policy may also imply that Australian companies are facing a low level of external threats as well as internal threats. Smith (1993) revealed a phenomenon: the threat of either a *consumer backlash* or of *legislative scrutiny* was often enough to spur a corporate examination of its policies. Smith (1993, p.116) stated "while a single consumer's concerns might be overlooked, the threat of extensive *negative publicity*, especially when it spurs a *legislative inquiry* or *pressure from a competitor*, can prompt immediate and rapt corporate attention." Therefore, there could be a low level of external threats in Australia.

Firstly, it may imply that there is a low level of threats from consumers. Many consumers may be accepting the current business activities of Australian organisations on the Internet. Or as people with positive attitudes towards organisations such as direct marketing are less concerned about privacy (Culnan and Milberg, 1999), Australians may have developed understandings towards the secondary use of personal information by organisations. However, consumers' attitudes on the Internet will be another area to be investigated as to further understand privacy issues.

Secondly, there is a low level of threats from Australian legislation, which does not cover private sector organisations since it only deals with the information handling practices of Commonwealth and ACT (Australian Capital Territory) government agencies. However, this study showed that some organisations in New South Wales follow the National Principles and proactively establishing a privacy policy. New South Wales involved in privacy issue by establishing Australian Privacy Charter Council as well as New South Wales Privacy Committee. Their conduct may influence the organisations in New South Wales, and it may imply that privacy can also be protected by high involvement of state governments in this issue. However, state governments may not act on this issue unless they face threats as well. Everyone seems to be reactive regarding privacy issue, in fact, many Australian organisations will probably not face external threats that force them to seriously ponder them.

Finally, there is a low level of threats from competitors. As appeared in this study, the majority of organisations have not acted on privacy issues. However, the study showed that a different level of pressure exits depending on industry sector. For example, 'Insurance' companies tend to have a privacy policy as they deal with confidential files on illness episodes of people. Also as the current Commonwealth Law provides privacy protection in area of Medicare and pharmaceutical benefits and medical research, 'insurance' companies have been pressured by legitimate bodies. On the other hand, although Commonwealth Law covers the area of tax file numbers, consumer credit reporting, spent convictions data-matching, not all 'financial and investment' companies that deal with these information have a privacy policy. In this study, no 'financial and investment' company has published a corporate privacy policy on the Internet.

The lack of a privacy policy may possibly indicate that there is no internal threat in Australia. That is, organisations are likely to consider that selected employees who have access to information collected on the Internet are acting ethically without any regulations, and will not invade the privacy of clients by misusing an authorised power on sensitive information. However, the research of Kamay and Adams (1993) indicates that employees continue to be an important financial threat in Australia. Trust enables people to take risks (Ratnasingham, 1998b). Organisations should minimise risks, thus, they should not wait till they face Internal threats.

Table 4.15 shows the summary of the research question 2 and question 3. These results must be viewed with limitations of this study in mind. In the following section, these are described.

Limitations of Study

The major problem of this search is the rapid growth of the Internet environment. The presence of undetected organisations could be found on the next day after the end of data collection stage of this research and/or the business activities and privacy policies of the organisations could be added.

Table 4.15: Summary of Question Two and Three

Question 2 Does it publish its privacy policy on the Internet or show concern for privacy protection?	□ Only 5.5 % of organisations on the Internet published its privacy policy. And they were all provided by Information Collectors. □ 4.1% of the sample organisations show their privacy concern. And they were shown by all Information Traders. Privacy concerns shown on the Internet are appeared to be technological protection. And they are ranked and listed as follows: 1. SSL technology 2. 128-bit encryption 3. User Authentication 4. Encryption of Stored Data 5. Tamper Proof data Transmission (eg, ISDN) 6. Secure access to Servers (eg Firewalls)
Question 3 How well is the privacy policy on the Internet established: does it meet the benchmark.	□ Poor privacy policies were found on the Internet, in fact, half of policies found show no intention to privacy protection. The other half of policies covered "use of disclosure' principles only.

Also, the final search (searching by entering guessed URL address: http://www.(company name).com.au) only relied on the name of the company itself. Although two search engines that identified the web sites containing the company name detect all associating sites of the company, the final search could not detect the companies that have a different trading name that resulted in limitation of this research.

Another problem of this research was its method of collecting privacy policies unavailable on the Internet. Gaining response often need incentives in order to encourage participants, however, such incentives were not included in this research.

Furthermore, the limitations to the above research underlie in several assumptions made by the researcher. Firstly, it must be pointed out that this research utilised a sampling method: it studied the top 100 private sector organisations in Australia. This study assumed the top 100 organisations based on market capitalisation as leading organisations. Although the large high-capitalised business like the sample used in this research showed low concerns on privacy protection on the Internet, it would be inappropriate to conclude that well-established privacy policies on the Internet are non-existent in all private sector corporations in Australia. It would be more accurate to study this topic by dividing organisations in smaller categories such as by industry and/or by state. Also, this research studied large organisations. Since the Internet provides the same opportunity for small businesses as well as individuals to do business on the Internet (Streeter et al., 1996), it is apparent that the Internet will be occupied by many small businesses. Without conducting the survey on small businesses on the Internet, it may not be appropriate to conclude that small businesses will follow the big business lead.

Secondly, this study assumed that organisations first establish policies to control their employees. This assumption has been made because the Privacy Commissioner has approached this matter by developing the national scheme in two stages, developing principles first and then moving onto the implementation issues (Scollay, 1998). Thus, it studied the quality of corporate privacy policies only. Organisations may control employees in different ways. Without establishing a privacy policy, organisations may be approaching this matter. For example:

- By carefully selecting a secure technology;
- By designing a physically and logically secure environment;
- By carefully selecting trusted employees;
- By educating employees to act ethically; and
- By monitoring employees' conducts.

The way of approaching this matter varies by organisations. Thus, the lack of privacy policy found in this study may not indicate anything about these other approaches.

Another assumption to this research was that 'National Principles for Fair Handling of Personal Information' meets best privacy practice. As these principles are the Australian Privacy Commissioner's recommended national approach (Scollay, 1998), these were utilised as a benchmark in this study. However, there are other guidelines available for organisations in privacy protection practice such as;

- □ Australian Privacy Charter developed by the Australian Privacy Charter Council;
- □ The Elements of Effective Self-regulation for Privacy Protection developed by Culnan (1998).

Everyone wants to avoid a patchwork of different standards, therefore, the government preferably approach this issue to provide national/international consistency in privacy standards. (Scollay, 1998)

Finally, the study classified the business use of the Internet into six categories: Non Internet Users, Information Providers, Information Collectors, On-line Traders, Restricted Traders and Under Contraction, and assumed that these are mutually exclusive. Similarly, the study classified privacy concerns of the organisations into three categories: No Concerns, Privacy Policy, and Privacy Concerns, and assumed they are mutually exclusive. It is certainly possible that a sample falls into more than one category.

However, these assumptions discussed above provided boundary in conducting this study. Therefore, the results obtained in this research present well within this boundary.

CHAPTER FIVE

CONCLUSION

In conclusion of this research, implications for organisations and Electronic Commerce are discussed. Also, recommendations for future research are discussed at the end of this chapter.

Implications for Organisations

Companies can gain competitive advantage by behaving ethically on the Internet. (Culnan and Armstrong, 1997). Organisations showing concern for privacy can lead to customers being willing to participate in the online trading. In fact, the majority of Internet users (77.5%) feel privacy is more important than convenience. (GVU's tenth WWW user survey, 1998). When considering privacy issues, it seems the question starts from 'what is sensitive information for individuals?' Sensitivity of information is difficult to determine as individuals have different levels. It seems to be advisable for organisations to handle any information about clients as sensitive information. "Any information clients send across the Internet should be private." (Pompili, 1996, URL: http://www.zdnet.com/pcmagazine). Therefore, organisations should consider the protection of entire information about clients. Three main factors must to be considered in privacy protection by organisations are described in the earlier section:

1. Corporate policies;
2. Corporate practices; and
3. Individuals' perceptions of their practices.

Firstly, corporate privacy policies should be placed on their trading sites. A survey conducted by Georgia Tech found that the majority (78.8%) of the survey participants would be willing to provide demographic information about themselves to the owner of a Web site if a statement was provided regarding how the information was used (cited in Culnan and Armstrong, 1997). A privacy statement that provides a clear guide for employees to ethically work on behalf of a organisations, and shows users how collected information is ethically treated, should be established in meeting the guidance of the Australian Privacy Commissioner, 'the National Principles for Fair Handling of Personal Information'. And these should be published on the Internet. It would allow clients to make a decision on participation. However, Marc Rotenberg, director of the Electronic Privacy Information Centre, said that the simple existence of privacy policies at Web sites does not indicate self-regulation is working (cited in Murphy, 1999a). Thus, organisations must ensure that actual practice meets the established policies.

In order to protect privacy of individuals, policies themselves are not sufficient. The IT department of each organisation must seek to reduce the risk of interception of communication, unauthorised access to records of communications, or to conceal the identities of the parties to a communication by implementing secure technology as well as implementing established policies. (Rotenberg, 1993) It makes it easier to describe the method of privacy protection at the organisational level according to the parties that access to information. Table 5.1 shows the summary of the method of privacy protection at the organisational level.

Table 5.1: Method of Privacy Protection at Organisational Level

Parties	Protection
Unauthorised – External	Technology: ISDN, Firewalls, Encryption
Unauthorised – Internal	1. Technology: Encryption, Password. 2. Policies
Authorised – Internal	Policies

Firstly, the security mechanism should be constructed using several technologies. The use of Firewalls and ISDN lines will certainly block external unauthorised access. Also the use of protocols such as S/MIME, DES, SET, SSL provide data security in transmission. Internal unauthorised access can be protected by storing data in encryption format and providing authorised parties strong password that nobody can guess. However, there is a limitation in obtaining privacy technologically. That is, there are always authorised parties who can access information. Privacy of individuals may be in the hands of those authorised parties: chosen persons within organisations and government.

Considerable steps must be taken in selection of authorised employees. Also employees' expectation should be clearly stated by organisations in the written form such as codes, policies, standards and rules. Although a code is viewed as a form or procedure that is looked at once and then filed, Codes of Ethics seem to have some effect on computer abuse judgements and intentions. (Harrington, 1996, p.272) Also, another important factor is that how well the established policies are implemented. Smith (1993) described various tactics that may be effective in implementing a policy such as formal penalties, incentives, social threat, control employee codes.

Finally, employee monitoring using new surveillance technology will be vital in controlling employees' behaviour at work. (Linowes, 1993) Although privacy of employees will be threatened, it is necessary in order to verify if employees are following corporate rules. George (1996) conducted a research on the topic of 'Computer-based monitoring' and concluded that,

> *"In some cases, computer-based monitoring is used in a punitive manner and contributes greatly to work-related illnesses. However, management can implement monitoring in such a way that employees do not only tolerate it but even approve of it, with low levels of associated work-related illnesses. Also management can manipulate the system and monitoring role within it such that increased pressure to produce can affect both work quality and employee health."*

Once organisations have developed strategies in privacy protection, it is necessary for organisations to gain the clients' trust. How can individuals trust those authorised people? It may not be possible especially in the environment of the Internet. According to Culnan and Armstrong (1997), individuals are less likely to perceive information collection procedures as privacy invasion under following circumstances:

- ❑ When information is collected in the context of an existing relationship;

- When they perceive that they have the ability to control future use of the information;
- When the information collected or used is relevant to the transaction; and
- When they believe the information will be used to draw reliable and valid inferences about them.

In addition, when individuals have the associated knowledge of organisational privacy practices as well as the capabilities of technologies, then they are more unlikely to meet an unexpected situation, hence feel less concerned. Table 5.2 shows a brief summary of what has been discussed in this section. The lists help organisations on the Internet to build a secure environment where clients can send any information without feeling insecurity.

Table 5.2: Recommendations for Organisations

1. Utilise technologies that block external as well as internal unauthorised parties' access;
2. Employ people who can follow corporate policies;
3. Educate people in technological and ethical aspects;
4. Establish corporate policies;
5. Implement corporate policies using incentives and penalties;
6. Monitor conduct of employees;
7. Notify monitoring procedures to employees;
8. Notify corporate practices to users.

Implications for Electronic Commerce

It is certain that all organisations are very interested in an increase of the use of the Internet for EC to fully take advantages of these technologies. According to Tara Lemmey, president and executive director of the Electronic Frontier Foundations, "speeding up the crucial processes of enabling users to set their own privacy boundaries and letting sites post privacy policies is critical to helping electronic commerce grow." (cited in Brooks, 1999). As described earlier, posting a privacy policy may affect clients' decisions on participation of EC. However, it is certain that clients are interested in how well the privacy policy is implemented. Since clients are unlikely to be notified of real practices of organisations in dealing their personal information, it seems that trust is an essential factor for EC. (Ratnasingham, 1998b)

Organisations' privacy practices are certainly a strong factor in developing trust between organisations and clients. Good privacy practices of organisations will certainly help clients trust their Internet dealings. In order to pressure organisations to behave ethically, three major sources must be involved. As described earlier, they are:

1. Government;
2. Consumers; and
3. Competitors.

Many organisations would not act on this issue unless a government requirement pressures them. Thus, the government involvement is vital in the development of EC. Secondly, as a consumer backlash often stimulates the conduct of organisations, Internet users could be involved in developing a secure Internet environment by continuously pressuring organisations as well as governments. People will not use the Internet until they trust the privacy capabilities of EC systems. However, it will only slow the development of a secure Internet world. The high involvement of Internet users is also essential in the development of EC.

Finally, Australian organisations should be more proactive in this issue. The result that the majority of Australian organisations are reactive in privacy issues may be slowing down the development of EC in Australia. Organisations have choices whether to collect information on the Internet. From a short discussion with one of sample organisations, it has become apparent that clients' contacts/requests increase when the site does not require specific personal information. Thus, some organisations are changing the form of business on the Internet from Information Collectors to Information Providers. Australian organisations can act as Information Providers until solutions to secure electronic transactions on the Internet are found. Otherwise, they often can be proactive in the development of EC systems by influencing companies and government to provide secure EC services.

Future Research

There are several recommendations for future research. As mentioned earlier, it would be more helpful to study this topic by dividing organisations in smaller categories such as by industry and/or by state. For example, this studied showed that many organisations in 'services industry' are proactively participating in online trading. The future research can investigate a specific industry in 'services industry'. It seems that 'financial and investment' companies are found to be proactively involved in On-line Trading. Therefore, the conduct of 'financial and investment' companies would be interesting for the future research. Also, the future research can investigate the 'good producing industry' since they have an opportunities in changing the way of doing business: to contact clients directly rather than going through 'wholesale' and/or 'retail trade' companies. Their further use of the Internet will be an interesting topic to look at. It should be interesting to investigate small businesses because it is possible that government will experience difficulties monitoring small organisations and individuals that enter into online trading. In addition to the business activities or privacy practices of small organisations and individuals, it would be interesting to identify legal knowledge of those people who open businesses on the Internet.

It is ideal that all organisations use all possible methods that provide maximum protection to personal information described in the earlier sections. Thus, the future research could look at various areas of organisational privacy protection practices such as:

- ❑ Technological protection in details that identify if organisations are using all described technologies that secure the information stored/transmitted on the Internet;
- ❑ Employees' ethics, awareness and perceptions of the corporate privacy policies. Even if a well-established corporate privacy policy is established, lack of employees' awareness and perception of those policies may result in ignoring policies. Thus, a study of ethics of employees may provide a good view of privacy protection practices; and

- ❑ Monitoring practices of organisations can provide how effectively monitoring is put in place to control employees' conduct.

Once the organisations are confidence in their practices, it will be interesting to study users' perception of those practices. Misunderstanding of organisations' practice often occurs even if organisations take reasonable steps to gain trust from customers. If customers perceive that the organisation's actual practice differs from what customers were told, this could result in customer dissatisfaction. Therefore, it is important for organisations to improve customers' knowledge of their real practices.

In addition to above recommendations, a study that covers the impact of privacy policy would be interesting. It is uncertain that the number of customers will increase by providing good privacy policy on the Internet. A simple survey was conducted by Georgia Tech (cited in Culnan and Armstrong, 1997, p.16) asking the Internet users a short question, "are you willing to provide demographic information about themselves to the owner of a web site if a statement was provided regarding how the information was used?" There is a difference between willingness and conduct. If it has no effect on users' participation in the Internet business, it is meaningless for organisations to publish their privacy policy without government requirement. The objective of organisations is to increase the number of customers by meeting their requirement. Therefore, it would be better to study the behaviour of customers. This can be studied using variables such as attractive price, product, brand, quality and/or convenience alike in the real world, or anonymous trade, secure trade, speed. It will be interesting to know what variable has high priority for customers. In another words, what factors make Internet users take high risks since the Internet today is known as an unregulated and insecure world? The Internet has created unusual conduct in both organisations and individuals. Thus, these conducts must be further studied in order to take full advantage of this technology.

REFERENCES

Agranoff, M. H. (1991). Controlling the Threat to Personal Privacy. *Journal of Information Systems Management.* Summer. pp.48-pp.52.

Angelides, M. C. (1997). Implementing the Internet for Business: A Global Marketing Opportunity. *International Journal of Information Management.* 17(6). pp.405-419.

Australian Bureau of Statistic. (1998). *Small Business in Australia 1996 - 1997.* Commonwealth of Australia. No.1321.0.

Bacard, A. (1995). *The Computer Privacy Handbook.* United States of America: Peachpit Press.

Barker, G. (1999, April, 12). ASIO Needs Power to Pry. *Australian Financial Review.* p.5.

Baum, D. (1996). Transcending EDI. *InfoWorld.* 19(12). pp.67-69.

Blank, S. C. (1984). *Practical Business Research Methods.* United States of America: The AVI Publishing Company Inc.

Bologna, J. (1991). A Framework for the Ethical Analysis of Information Technologies. *Computers & Secur*ity. 10(4). pp.303-307.

Bridis, T. (1999, 12 May). Study:Web Sites Privacy Improves. Inforwar.com. URL: http://www.inforwar.com/class_1/99/classl_051299b_j.shtml. (cited on 12/6/99).

Brooks, R. (1999). Which Australian Web Sites Care About Your Privacy. URL: http://www.abaconsulting.com.au/prirvacyart.htm. (Cited on 5/6/99).

Clarke, R. (1994). The Digital Persona and its Application to Data Surveillance. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html. (Cited on 18/6/98).

Clarke, R. (1996). Federal Privacy Legislation in Australia. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/FedLeg.html. (Cited on 18/6/98).

Clarke, R. (1997a). Data Surveillance and Information Privacy. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/. (Cited on 3/3/98).

Clarke, R. (1997b). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html. (Cited on 3/3/98).

Clarke, R. (1997c). Privacy on the Internet, Threat, countermeasures and Policy. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/Internet.html. (Cited on 16/3/98).

Clarke, R. (1997d). Promises and Threats in Electronic Commerce. URL: http://www.edu.au/people/Roger.Clarke/EC/Quantum.html. (Cited on 3/3/98).

Clarke, R. (1998a). A Primer on Internet Technology. URL: http://www.anu.edu.au/people/Roger.Clarke/II/IPrimer.html. (Cited on 13/6/98).

Clarke, R. (1998b). Technological Aspects of Internet Crime Prevention. URL: http://www.anu.edu.au/people/Roger.Clarke/II/ICrimPrev.html. (Cited on 13/6/98).

Clarke, R. (1998c). Message Transmission Security (or 'Cryptography in Plain Text'). URL: http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html. (Cited on 18/6/98).

Collin, S. (1997). *Setting Up a Web Server.* United States of America: Digital Press.

Cooper, D. R. and Emory, C. W. (1995). *Business Research Methods.* 5th Edition. United States of America: Irwin.

Cravens, D. W. (1994). *Strategic Marketing.* 4th Edition. United States of America: Irwin.

Cronin, M. J. (1995). *Doing More Business on the Internet – How the Electronic Highway is Transforming American Companies.* United States of America: Van Nostrand Reinhold.

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information. *MIS Quarterly.* 17(3). pp.341-363.

Culnan, M. J. (1998). A Methodology to Assess the Implementation of the Elements of Effective Self-Regulation for Protection of Privacy. Paper Prepared for the National Telecommunications Information Agency. U. S. Department of Commerce. URL: http://www.gsb.georgetown.edu/dept/facserv/work/mis.html.

Culnan, M. J. and Armstrong, P. K. (1997). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. URL: http://www.gsb.georgetown.edu/dept/facserv/work/mis.html.

Culnan, M. J. and Milberg. S. J. (1999) Consumer Privacy. URL: http://www.gsb.georgetown.edu/dept/facserv/work/mis.html.

Dahl, A. and Lesnick, L. (1996). *Internet Commerce.* United States of America: New Riders Publishing.

Davidson, J. (1999a, 19 January). Australia: Cryptography Cyber Treaty Will Have No Effect – Expert. *The Australian Financial Review*. URL: http://www.infowar.com/class_1/99/class1_020399b_j.shtml.

Davidson, J. (1999b, 30 April), Australia: Secret IT Business. *The Australian Financial Review*. p.38.

Deans, P. C. and Kane, M. J. (1992). *International Dimensions of Information Systems and Technology*. United States of America: Pws-kend Publisher.

Dixon, T. (1995). Privacy Charter Sets New Benchmark in Privacy Protection. Privacy Law & Policy Reporter. URL: http://www.austlii.edu.au/do2/disp.pl/au/other/plpr/Vol2No03/v02n03a.htm. (Cited on 30/4/98).

Doddrell, G. R. (1995). Information Security and the Internet. *Information Management & Computer Security*. 3(4). pp.15–19.

Dwyer, T. (1994). Privacy Implications of New Communications: Networks and Services. URL: http://www.austlii.edu.au/hreoc/privacy/newcomms.htm. (Cited on 19/3/99).

Emmelhainz, M. A. (1990). *Electronic Data Interchange*. New York: Van Nostrand Reinhold.

Emory, W. (1985). *Business Research Methods*. 3rd Edition. United States of America: IRWIN.

Foo, S. and Lim, E. P. (1997). Managing World Wide Web Publications. *Information Management & Computer Security*. 5(1). pp.11–17.

Foo, S., Leong, P. C., Hui, S. C. and Liu, S. (1999). Security Considerations in the Delivery of Web-based Applications: a Case Study. *Information Management & Computer Security*. 7(1). pp.40–49.

Forcht, K. A. and Wex, R. (1996). Doing Business on the Internet: Marketing and Security Aspects. *Information Management & Computer Security*. 4(4). pp.3–9.

Ford, P. (1996). Information Security, Censorship and Privacy. URL: http://www.anu.edu.au/people/Roger.Clarke/II/Ford960619.html. (Cited on 12/6/98).

Garfilkel, S., and Spafford, G. (1997). *Web Security & Commerce*. United States of America: O'Reilly & Associates, Inc.

George, J. F. (1996). Computer-Based Monitoring: Common Perceptions and Empirical Results. *MIS Quarterly*. 20(4). pp. 459-488.

Ghauri, P., Gronhaug, K. and Kristianslund, I. (1995). *Research Methods in Business Studies: A Practical Guide*. Great Britain: Prentice Hall Europe.

Gluck, F. B. (1994). Protection of Electronic Mail and Electronic Messages: Challenges and Solutions. *Information Management & Computer Security.* 2(1). pp.28–40.

Gore, S. (1996). EDI over the Internet. URL: http://www.niit.org/what/reptatspeech/reports/edi.html. (Cited on 16/3/98).

GVU's Tenth WWW User Survey (October 1998). URL: http://www.gvu.gatech.edu/user_surveys/ (Cited on 15/7/99).

Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly* 20(3). pp.257-278.

Head, B. (1998, January 9). On Alert for Hack Attack. *The Australian Financial Review.* p.16.

Hochheiser, H. (1996). Electronic Privacy Guidelines. URL: http://www.netaction.org/privacy/guidelines.html. (Cited on 16/3/98).

Jilovec, N. (1997). The Cost of Doing EDI. *MIDRANGE systems.* 10(8). pp.22.

Kamay, V., and Adams, T. (1993). The 1992 Profile of Computer Abuse in Australia: Part 2. *Information Security Management & Computer Security.* 1(2). pp.21–28.

Kathleen, M. (1999, 17 May). Survey Finds Most Sites Post Privacy Policies. Internet World. URL: http://www.internetworld.com/print/1999/05/17/news/19990517-survey.html. (cited on 12/6/99)

Kelin, D. B. and Goodhue, D. L. (1997). Can Humans Detect Errors in Data? Impact of Base Rates, Incentives, and Goals. *MIS Quarterly.* 21(2). pp.169-194.

Kervin, J., B. (1992). *Methods for Business Research.* United States of America: Harper Collins Publishers Inc.

Kling, R. (1996). Beyond Outlaws, Hackers, and Pirates: Ethical Issues in the Work of Information and Computer Science Professionals. In R. Kling (Ed.). *Computerization and Controversy – Value Conflicts and Social Choice* (2nd Edition). pp.848-869. London: United Kingdom.

Lacovou, C. L., Benbasat, I. and Dexter, A. S. (1995). Electronic Data Interchange and Small Organisations: Adoption of Impact of Technology. *MIS Quarterly.* December. pp.465–482.

Lane, E. and Summerhill, C. (1993). *Internet Primer for Information Professionals: A Basic Guide to Internet Networking Technology.* United States of America: Meckler Publishing.

Laudon, K. (1996). Markets and Privacy. In R. Kling (Ed.). *Computerization and Controversy – Value Conflicts and Social Choice* (2nd Edition). pp.697–726. London: United Kingdom.

Lawrence, M. (1998). Little Brother is Watching. *InformationWeek.* 669. pp.146.

Leedy, P. D. (1997). *Practical Research – Planning and Design.* 6th edition. United States of America: Prentice-Hall.

Linowes, D. F. (1993). Your Personal Information has Gone Public. In R. Kling (Ed.), *Computerization and Controversy – Value Conflicts and Social Choice* (2nd Edition). pp.637-642. London: United Kingdom.

Lorek, L. A. (1997). Business, Government, even Homes Open to PC Criminals. URL: http:// www.kentuckyconnect.com/heraldleader/news/101997/fpccrime.html. (Cited on 25/2/98).

Lynch, D. C. and Rose, M. T. (1995). *Internet System Handbook.* United States of America: Addison-Wesley Publishing Company.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly.* 10(1). pp.4–12.

McElroy, D. and Turban, E. (1998). Using Smart Cards in Electronic Commerce. *International Journal of Information Management.* 18(1). pp.61–72.

Milberg, S. J., Burke, S. J., Smith, H. J. and Kallman, E. A. (1995). Values, Personal Information, Privacy, and Regulatory Approaches. *Communication of the ACM.* 38(12). pp.65-74.

Murphy, K. (1999a). Newsmaker: Mary Culnan. URL: http://www.internetworld.com/print/1999/03/08/news/publish.html. (Cited on 7/27/99)

Murphy, K. (1999b). Survey Finds Most Sites Post Privacy Policies. URL: http://www.internetworld.com/print/1999/05/17/news/1990517-survey.html. (Cited on 7/27/99)

Nath, R., Akmanligil, M., Hjelm, K., Sakaguchi, T. and Schultz, M. (1998). Electronic Commerce and the Internet: Issues, Problems, and Perspectives. *International Journal of Information Management.* 18(2). pp.91–101.

Ng, H., Pan, Y. J. and Wilson, T. D. (1998). Business Use of the World Wide Web: A Report on Further Investigations. *International Journal of Information Management.* 18(5). pp.291-314.

O'Connor, K. (1995). Community Attitudes to Privacy. URL: http://www.austlii.edu.au/hreoc/privacy/commun.htm. (Cited on 3/3/98).

OECD. (1997) URL: http://www.oecd.org. (Cited on 3/3/98).

Pattison, M. (1997). Legal Implications of Doing Business on the Internet. *Information Management & Computer Security.* 5(1). pp.29–34.

Pompili, T. (1996). Evolving Internet Security Methods. PC Magazine Online. URL: http://www.zdnet.com/pcmagazine. (Cited on 16/3/98).

Privacy Commissioner. (1995). Sixth Annual Report on the Operaton of the Privacy Act for the Period of 1 July to 30 June 1994. Canberra: Australian Government Publishing Service.

Privacy Commissioner. (1998). Obligations under the Privacy Laws. URL: http://www.austlii.edu.au/hreoc/privacy/privacy.htm. (Cited on 3/3/98).

Privacy Commissioner. (no date). What is Information Privacy and Why Do We Need to Protect It? URL: http://www2.austlii.edu.au/itlaw/national_scheme/national-PART.html. (Cited on 3/3/98).

Privacy Protection in the Private Sector. (1996). URL: http://www.agps.gov.au/customer/agd/clrc/privacy.htm. (Cited on 3/3/98).

Radosevich, L. (1996). The once and Future EDI. URL: http://www.cio.com/forums/ec/ec_future_edi.html. (3/3/98).

Ratnasingham, P. (1998a). Internet-based EDI Trust and Security. *Information Management & Computer Security.* 6(1). pp.33–39.

Ratnasingham, P. (1998b). Trust in Web-based Electronic Commerce Security. *Information Management & Computer Security.* 6(4). pp.162–166.

Renton, N. E. (1997). *Public Relations, Newsletters and Internet Usage for Organisations.* Australia: Kangaroo Press.

Rotenberg, M. (1993). Communications Privacy: Implications for Network Design. *Communication of the ACM.* 36(8). pp.61-73.

Rubin, A. D., Geer, D. and Ranum, M. J. (1997). *Web Security Sourcebook.* United States of America: John Wiley & Sons.

Rutrell, Y. (1998). The Next Level. *InternetWeek.* 699. pp.47–50.

Schermerhorn, J. R. (1992). *Management for Productivity.* 3rd Edition. United States of America: John Wiley & Sons.

Schneier, B. (1998). Security Pitfalls in Cryptographic Design. *Information Management & Computer Security.* 6(3). pp.133–137.

Scollay, M. (1998). National Principles for the Fair Handling of Personal Information. (1998). URL: http//:www.austlii.edu.au/privacy/privacy.htm. (Cited on 16/6/98).

Senn, J. A. (1995). *Information Technology in Business Principles, Practices, and Opportunities.* United States of America: Prentice Hall.

Shattuck, J. (1984). Computer Matching is a Serious Threat to Individual Rights. In R. Kling (Ed.), *Computerization and Controversy – Value Conflicts and Social Choice* (2nd Edition). pp.645-658. London: United Kingdom.

Sillince, J. A., MacDonald, S., Lefang, B. and Frost, B. (1998). Email Adoption, Diffusion, Use and Impact within Small Firms: A Survey of UK Companies. *International Journal of Information Management.* 18(4). pp.231–242.

Sipior, J. C., and Ward, B. T. (1995). The Ethical and Legal Quandary of Email Privacy. *Communications of ACM.* 38(12). pp.48–54.

Smith, H. J. (1993). Privacy Policies and Practices: Inside The Organizational Maze. *Communication of the ACM.* 36(12). pp.105–122.

Smith, H. J., Milberg, S. J. and Burke, S. J. (1996). Information Privacy: Measuring Individual's Concerns About Organizational Practice. *MIS Quarterly.* 20(2). pp.167–195.

Straub, D. W. and Collins, R. W. (1990). Key Information Liability Issues Facing Manager: Software Piracy, Proprietary Databases, and Individual Rights to Privacy. *MIS Quarterly.* 14(2). pp.143–156.

Streeter, L. A., Kraut, R. E., Lucas, H. C. and Caby, L. (1996). How Open Data Networks Influence Business Performance and Market Structure. *Communications of ACM.* 39(7). pp.63-73.

The Australian Privacy Charter. (n.d.). URL: http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html. (Cited on 18/6/98).

Thomson, M. E. and Solms, R. V. (1998). Information Security Awareness: educating Your Users Effectively. Information Management and Computer Security. 6(4). P.167-173.

Tucker, M. J. (1997). EDI and the Net: A profitable Partnering. *Datamation.* April. 42(4). pp.62-67.

Washburn, D. and Tauber, E. (1997, 17 August). Internet is Significant Threat to Personal Privacy. Privacy on the Internet. URL: http://www.mcall.com/special/privacy/pri1.htm. (cited on 6/6/98).

Wearne, P. (1998, August 2). Public Servants in Net-porn Rort. *Sunday Times.* p.1-2.

Webler, R. P. (1990). *Basic Content Analysis*, 2nd Edition, United States of America: SAFF Publications.

Weisband, S. P. and Reinig, B. A. (1995). Managing User Perceptions of Email Privacy. *Communications of the ACM.* 38(12). pp.40-47.

Wilson, S. (1997). Certificates and Trust in Electronic Commerce. *Information Management & Computer Security*. 5(5). pp.175–181.

Wolinsky , C. and Sylvester, J. (1992). Privacy in the Telecommunications Age. *Communications of the ACM*. 35(2). pp.23–25.

Woodman, R. W., Ganster, D. C., McCuddy, M. K., Tolchinsky, P. D. and Fromkin, H. (1982). A Survey of Employee Perceptions of Information Privacy in Organizations. *Academy of Management Journal*. 25(3). pp.647-663.

Zgodzinkski, D. (1997). Click here to Pay. *Internet World*. September. 8(9). pp.60-67.

Zikmund. W. G. (1991). *Business Research Methods.* 3rd Edition. United States of America: Dryden Press.

APPENDICES

1. Observation Checklist

PART I: Demographic Data		
Rank		
Size *		
State *		
Industry *		
PART II: Business Use on the Internet		
1. Have WWW Address □ What is the address? ____________________	Yes Go to 2	No (Class 1)
2. Does it publish various information on organisations and products/services	Yes Go to 3	No Go to 5
3. Does it collect personal information (Name, Home Address, Home Phone Number)	Yes Go to 4	No (Class 2) Go to 7
4. Does it collect Credit Card Number	Yes (Class 4) Go to 7	No (Class 3) Go to 7
□ Sent a Letter requesting a Privacy Policy. □ Date: / /	Received	No Reply
□ Send a reminder. □ Date: / /	Received	No Reply
5. Does it prohibit access without an original browser (Organisations Use Only)?	Yes (Class 5)	No Go to 6
6. Does it show "Under-construction" messages? □ Provide details. ____________________ ____________________	Yes (Class 6)	No
PART III: Privacy Policy on the Internet		
7. Does it publish a privacy policy □ Attach the privacy policy.	Yes (Class 3)	No Go to 8
8. Is there any statements on privacy or security of personal information □ Attach the statement. □ Attach other statement provided on the Internet.	Yes (Class 2)	No (Class 1)

* *See Section: Data Analysis for Classification.*

2. Request Letter Sent to the Sample Organisations

EDITH COWAN
UNIVERSITY
PERTH WESTERN AUSTRALIA
CHURCHLANDS CAMPUS

Keiko Sato
School of MIS, Churchlands Campus, Western Australia, 6018
Tel:
Fax:
Email:

FACSIMILE MESSAGE

TO		ORGANISATION	
	COUNTRY	AREA CODE	NUMBER
FROM Keiko Sato	TIME	DATE	NO. PAGES (including this one) 1

MESSAGE

I am a masters student at Edith Cowan University in WA conducting research on Corporate Privacy Policy in handling clients' information on the Internet.

Could you please inform me if you have general privacy policy? Also, does your organisation have a specific policy for Internet dealings? If you have either of these, is it possible for me to view them?

If you require any more information on this research please contact
myself, or my supervisor:

Dr W Hutchinson
Associate Head of School of Management Information Systems
Edith Cowan University
Churchlands
Western Australia 6018
Tel: (
Email: ______________________

Thanks you for your assistance.

Regards

Keiko Sato

3. Evaluation Sheet

Evaluation Checklist
National Principles for the Fair Handling of Personal Information

Collection	
□ We will only collect information that is necessary for what we do.	
□ We will only be fair in the way we collect information about you.	
□ We will tell you who we are and what we intend to do with information about you.	
□ Where practicable, we will collect personal information directly from you.	
□ If we collect information about you from someone else we will, wherever possible, make sure you know we have done this.	
Use and Disclosure	
□ We will only use or disclose information about you in ways that are consistent with your expectations or are required in the public interest.	
Data Quality	
□ We will ensure that information about you is accurate when we collect or use it.	
Data Security	
□ We will keep information about you secure.	
Openness	
□ We will be open with you about what kinds of personal information we hold and what we do with it.	
Access and Correction	
□ Wherever possible we will let you see the information we hold about you and correct it, if it is wrong.	
Identifiers	
□ We will limit our use of identifiers that government agencies have assigned to you.	
Anonymity	
□ If we can (and you want to) we will deal with you anonymously.	
Trans-border Data Flows	
□ We will take steps to protect your privacy if we send personal information about you outside Australia.	
Sensitive Information	
□ We will limit the collection of highly sensitive information about you.	