Privacy Issues on the Internet

Winnie Chung and John Paynter
Department of Management Science and Information Systems
School of Business, The University of Auckland
Private Bag 92019, Auckland, New Zealand
winniec@ihug.co.nz; j.paynter@auckland.ac.nz

Abstract

An increasing number of people are using the Internet, in many instances unaware of the information being collected about them. In contrast, other people concerned about the privacy and security issues are limiting their use of the Internet, abstaining from purchasing products online.

Businesses should be aware that consumers are looking for privacy protection and a privacy statement can help to ease consumers' concerns. New Zealand based web sites are expected to have privacy statements on their web sites under the New Zealand Privacy Act 1993. The incidence of the information gathered from New Zealand web sites and their use of privacy statements is examined here. In particular, web sites utilizing cookies and statements about them are scanned.

Global consistency on Internet privacy protection is important to boost the growth of electronic commerce. To protect consumers in a globally consistent manner, legislation, self-regulation, technical solutions and combination solutions are different ways that can be implemented.

1. Introduction

The Internet is an amazing tool now being widely used. It has the potential to change the way people live. With only a few mouse clicks, people can follow the news, look up facts, buy goods and services, and communicate with others from around the world. However, the power of the Internet also allows for the efficient, inexpensive collection of vast amounts of information. People can give away information about themselves if they are not careful. The prevalence, ease, and relative low cost of such information collection distinguish the online environment from a more traditional means of commerce and information collection. This raises consumers' concerns regarding threats to their personal privacy whilst online. The issues of information privacy on the web need to be considered.

The Internet is international and largely unregulated. This means that the laws of any one country do not usually apply to Internet activities originating in other countries. Thus, it is necessary to discuss how privacy protection could be achieved in a globally consistent manner.

2. Internet privacy

Warren and Brandeis [1] defined privacy as the “right to be let alone”. Information privacy exists when the usage, release and circulation of personal information can be controlled [2]. Invasions of privacy occur when individuals cannot maintain a substantial degree of control over their personal information and its usage [3]. The growth of the Internet with the rapid advance of technology raises consumers' concerns regarding threats to their personal privacy whilst online.

2.1 Why there are Internet Privacy concerns?

The Internet allows for the efficient, inexpensive collection of information without consumers' consents. It can track consumers in unique ways whether or not a consumer is aware of it. This includes consumer's preference, interest or even credit card information.

Federal Trade Commission (FTC) conducted a study in March 1999 [4]. It discovered that 92.8 percent of web sites were gathering at least one type of identifying information (name, e-mail address, postal address), while 56.8 percent were collecting at least one type of demographic information (gender and preferences). The monetary value of this information explains why so many web sites gather personal information. This raises consumers' concern about their privacy rights. Consumers worry about the security of their personal information and fear that it may be misused. They are

0-7695-1435-9/02 $17.00 (c) 2002 IEEE

concerned about how their personal information may be treated now or in the future after it has been collected.

2.2 What are the concerns?

The privacy threats of which people are concerned include:

- Visits to web sites will be tracked secretly.
- E-mail addresses and other personal information will be captured and used for marketing or other purposes without permission.
- Personal information will be sold to third parties without permission.
- Credit card theft

The advances of Internet and database technology increase information privacy concerns. Data entered into forms or contained in existing databases, can be combined almost effortlessly with transaction records and records of an individual's every click of a mouse on the Internet. Privacy concerns increase further as data mining tools and services become more widely available.

Cookies are now widely used to identify users at a web site, some people consider this to be privacy invasive. The user will be prompted for information such as gender, age, buying preferences or even email address. For example, one will be prompted to enter email address, billing address and other information if one wants to buy a book from Amazon.com. The information will be packaged into a cookie and sent to the user's hard drive, which stores it for later user identification. The user's browser will send the cookie to the web server when the user goes to the same web site. The web server can utilise the information in the cookie to generate customised web pages according to the interests and preferences of the user. In fact, information about one's movement in a web site can also be stored in a cookie. The main concern is that all this is done without one's knowledge.

By using cookies, businesses can obtain personal information such as buying habits, e-mail address or the portions of web site that were looked at previously. This information can be combined into mailing lists for direct marketing purposes or it can be sold to third parties. For example, America Online shares information about its users with various partners, including companies that do direct mailing and telephone solicitations [5].

A web bug is another widely used instrument that poses a threat using online tracking technology. Some people find it is invasive to their privacy when they are visiting a web site. Web bugs are invisible pieces of code that can be used for several purposes, from secretly tracking people's web travels, to pilfering computer files [19]. The simplest form of web bug is a small graphic interchange format that can work and match with cookies to send information to third parties about a visitor's online travels. An executable bug can install a file onto people's hard drives to collect information whenever they are online. A script-based executable bug can be installed on a user's computer that can take any document from the user's computer without notice. Another form of script-based executable bug is based on servers. They can track visitor's travels on the web and control the person's computer from its server. For example, it launches multiple browser windows when a person tries to exit the site.

Many web sites and net advertising companies place web bugs on their pages to collect information, such as which pages are being read most often. As mentioned earlier, the bugs can be used in a more invasive way, for example, to capture a visitor's Internet Protocol address or installing pernicious files in the visitor's hard drive. The concern is that with a web bug, the visitor's computer can be fully exposed to malicious sites that can take any files or information from programs on the visitor's hard drive without their knowledge and consent. A report shows that 16 million pages out of 51 million that were scanned contain at least one web bug that had been attached from a third party, such as an advertising network [19]. When web bugs are used maliciously, the computer user's entire e-mail address book can be stolen without notice merely by clicking on a bugged web page.

Another privacy concern is that marketers can match their customer databases with the databases they get from the cookies. DoubleClick had already built up a database of online consumers' browsing habits by using cookies. It paid Abacus Direct Corporation. $1.7 billion for the list of catalogue purchasers' names and addresses [6]. This allows cross-referencing that matches information with real world names, addresses and histories of offline mail order purchases [7]. The acquired names and addresses can be linked with the cookies so DoubleClick not only knew where people are online, but where they live, who they are, and their phone numbers. This could be the most comprehensive customer database in the world that can be used for direct marketing purposes.

There is a potential for fraudulent activities on the Internet, as few regulatory standards exist [8]. The security of credit card information for online purchases is incorporated with the privacy concerns. Bibliofind, a subsidiary of Amazon.com admitted that hackers undetected over four months have stolen 98,000 credit card numbers. Hackers from time to time like to publish a list of stolen credit card numbers and other related information on the Internet. The disclosure of credit card information without permission may lead to credit card fraud, which is another consumer concern.

3. Arguments against Internet Privacy concerns

To some people, Internet privacy concerns are not special issues, and some are just over sensitive as they realise that the Internet is growing. In fact, shopping online is not different from in-store shopping. They both raise the same privacy concerns. Tracking a person's navigation while online can be compared to a camera spying on people while they are moving around in a store.

Although cookies can be used to identify users to a web site, in fact they cannot find out names, addresses, and other personal information unless consumers have provided such information voluntarily [6]. Thus, the use of cookies is not a main point regarding the privacy concerns. In fact, some people are willing to give away their personal information in return for discounts and other particular benefits [25]. The use of cookies for online purchases is not different from catalogue purchases by mail when personal information is provided voluntarily. They both raise the same privacy concerns that information may be misused when it gets to the hand of the businesses.

Another argument emphasises that Internet privacy concerns are trivial. Consumers do not want to reveal their information online for marketing purposes. Actually consumer information can also be found in telephone books or other sources. This information can usually be used by marketers for marketing promotions. Marketers can send flyers to physical letterboxes based on this information. It is argued that getting rid of junk email is easier than getting rid of junk physical mail. Thus, the privacy concerns regarding junk email are considered to be trivial.

In addition, some web sites collect personal information but never use it. For example, Steinlager is a New Zealand web site that offers competitions to visitors. It is mentioned in the web site that information obtained will be used for marketing purposes. This site was studied as part of a previous project [11], however, the information until now has not been used for any form of direct marketing. It is not really a concern when obtained information is not being used.

4. Arguments for Internet Privacy concerns

Although the previous section provides several arguments that suggest Internet privacy concerns are not a special concern, it is a good idea for a web site to consider this issue. Consumers are really interested in the safeguard of their privacy. Surveys show that the primary reason most non-Internet users avoid the Internet is because of the concern about the privacy and safety of their personal information and communications [9]. Privacy concerns prevent some consumers from buying products on the web. A marketing research firm, NFO Interactive, conducted a study in 1999 and found that almost three out of four consumers who browse the Internet never make any purchases online [5]. Those consumers said that they would be more likely to buy if they could be assured that their privacy would be respected [5]. A recent study on the travel sector in New Zealand also suggests that privacy and security are the concerns that stop people purchasing travel ticket online [20].

Although personal information may not be used after collection, it must be noticed that collecting and keeping this information is a potential liability for a web site when it meets some consumers that take the safeguard of their privacy seriously. Internet based businesses should care about the privacy concerns because consumers care about it. Since businesses are developing relationships with consumers, it helps if consumers know that businesses care about them. Surveys show that people are more comfortable if they see a privacy statement, and are more assured if a privacy statement has been approved by a third party, such as TrustE [10, 24]. To boost the development of e-commerce, information privacy concerns should be treated seriously as they are discouraging consumers from using the Internet in buying goods and services.

5. The New Zealand Privacy Law

New Zealand's Privacy Act 1993 does not create a right of privacy nor is its recognition of privacy interests absolute [12]. Its coverage includes both electronic and paper information. Any business based in New Zealand wishing to engage in electronic commerce with consumers must ensure its activities comply with the Privacy Act, to the extent that they involve personal information about their consumers. Personal information includes any information about an identifiable living person, whether it is on a computer, in a paper file or in someone's head [12]. The Privacy Act applies to the handling of all personal information collected or held by agencies, whether in the public or private sectors [12].

In New Zealand, consumers' privacy concerns can largely be met through businesses complying with the Privacy Act. To comply with information privacy principle 3 of section 6 of the Privacy Act 1993, New Zealand web sites that collect personal information should include a privacy statement that sets out the purpose of the collection and the uses and any disclosures that may be made of that information [13].

6. Web site Privacy Statements

In New Zealand, Information privacy principle 3 sets out how a web site goes about collecting information from someone. Companies are required to alert people to a number of matters when information is collected from them [14]. The matters include:

- The fact of collection.
- The purpose of collection.
- Intended recipients of the information.
- Contact details for the company collecting and the company holding the information.
- If the collection is authorised or required by law - the particular law and whether supplying the information is voluntary or mandatory.
- Consequences for people if all or part of the information is not provided.
- People's rights of access to, and correction of, personal information.

A well-expressed web site should have a privacy statement and the statement should meet the requirements of principle 3. Thus, matters can be drawn to people's attention before the information is collected. Compliance with principle 3 can help to build the trust between businesses and consumers. Policy that provides consumers with more control will reduce consumer concerns [6].

6.1 Addressing privacy on overseas web sites

Slane [14] mentioned the results of surveys conducted in Hong Kong and United States in 1998. The Privacy Commissioner for Personal Data in Hong Kong conducted a survey of web sites. The results indicated that although 63.8 percent of the web sites surveyed provided forms to collect personal data, only 31.9 percent had statements notifying people of the purposes for collecting the personal data, and only 6 percent had a privacy policy statement [14]. In 1999, the result showed improvement but there is still some way to go. 77 percent of web sites notified people of the purposes for collecting the information and 23 percent had a privacy policy statement [14].

In 1998, the FTC in the United States examined the practice of 1,400 commercial sites on the web. Although 85 percent of the sites surveyed collected personal information from consumers, only 14 percent provided any notice of the purpose of collection, and only 2 percent provided notice by way of a comprehensive privacy policy [14]. The above results show that personal information is being collected from web sites, most of which do not have a comprehensive privacy policy.

6.2 Addressing privacy on New Zealand web sites

Many New Zealand web retailers are not providing enough information to safeguard consumer rights [22]. New Zealand consumers have the same rights irrespective of whether the transaction is carried out electronically or by traditional means [23]. People increasingly expect to find a privacy statement at web sites. New Zealand based businesses should be warned that privacy concerns need to be treated seriously. In New Zealand, web site privacy statements are expected under information privacy principle 3 [13]. No published survey has been conducted to ascertain the level of compliance with principle 3 by New Zealand based web sites [14]. In this paper, 140 New Zealand based web sites were chosen to evaluate the degree of privacy issues being handled by these sites. The 140 web sites were chosen as the best-known ones from different sectors. The sectors are classified as banking, travel, car, e-tailer, franchise, sports, fashion, farming and others.

A coding sheet was used to record the presence or absent of attributes for each web sites. Each row represents a web site and each column indicates an attribute. There are three attributes in the coding sheet. Each web site was recorded whether it collects any personal data in any form including cookies, whether it notifies people the purpose for collecting the data, and whether it notifies people by a privacy policy statement.

Some sites were so large and disparate in nature (e.g. the universities and local bodies) that it was difficult to find whether or not they included a privacy statement, especially where they did not include a search facility. For instance, one part of the site (a public library), might have a privacy statement but it was lacking from the overall site. Where the presence or absence of a privacy statement could not easily be ascertained, then the site is not included in the survey. Table 1 shows the results for different sectors:

Sector	Number of sites	Collect personal data	Notify purpose for collecting	Notify by a privacy statement
Banking	9	100%	44%	33%
Travel	7	57%	25%	25%
Car	14	50%	14%	14%
E-retailer	13	100%	69%	62%
Franchise	18	83%	27%	13%
Sports	15	33%	40%	20%
Fashion	5	80%	0%	0%
Farming	11	55%	67%	83%
Others	48	63%	50%	47%

Table 1: Analysis of web site privacy statements

As shown in Table 1, all sites in the banking sector collected personal data, 44 percent provided notice of the collection purpose and 33 percent provided a privacy policy. 57 percent and 50 percent of the sites from the travel and the car sectors respectively, collected personal data. Only 25 percent and 14 percent of travel and banking sites respectively, provided notice of the collection purpose and those provided privacy statements. 100 percent of the e-tailer sites collected personal data and within those, 69 percent notified the purpose of collection and 62 percent notified by a privacy statement. For the franchise sector, 83 percent of sites collected personal data. However, only 27 percent provided notice of the collection purpose and only 17 percent notified by a privacy statement. 33 percent and 80 percent collect personal data for the sports and fashion sector respectively. 40 percent from the sports sector notified purpose of collection and 20 percent provided by a privacy statement. However, the fashion sector sites did not make any notification regarding information collection.

It is interesting that in the sports sector the percentage that notifies the collection purpose (40 percent) is more than the percentage that collects personal data (33 percent). The reason is because some web sites in the sport sector claim that they do collect personal data but in fact they do not. The same phenomenon appears in the farming sector. Only 55 percent of farming sites collect personal data but 67 percent notify the purpose of collection and 83 percent even provide a privacy statement.

The results for different sectors indicate that they were not uniform in respecting consumers' privacy by providing notification of the information collecting purposes. For instance, it is interesting that although a large proportion of sites in the fashion factor collected personal data, no notice is being given regarding information collection. In contrast, for the travel and car sectors, those sites that notified the purpose of collection tend to provide a privacy policy. That is, if sites consider privacy concerns, they will have an explicit privacy policy rather than just notifying people without any comprehensive statement.

In general, 66 percent of the 140 studied web sites collected some sort of personal data from consumers. Within those that collected personal information, 43 percent notified the purpose of collection and 38 percent provided notice by a way of a comprehensive privacy statement. The difference between those that provided any notice of the purpose of collection and those that provided notice by way of a comprehensive privacy statement is only 5 percent. This implies that most web sites that considered the privacy concerns tend to notify people the purpose of collecting their personal information with a privacy statement; otherwise, web sites simply ignored consumers' privacy without having any notification of the collection purposes. This also denotes that some web sites simply use comprehensive privacy statements as a border plate. In any case, having a comprehensive privacy statement is beneficial to a web site as this makes most visitors feel more positive or confident about the web site [25].

The above results indicate that New Zealand based web sites collected personal data as overseas web sites do. Some New Zealand web sites consider privacy concerns and show that they treat the issue seriously. However, further improvement is still needed if New Zealand web sites want to ease consumer's privacy concerns.

7. Mechanism for addressing privacy issues

The Internet is international and largely unregulated. This means that the laws of any one country do not usually apply to Internet activities originating in other countries. All countries do not implement laws regarding Internet privacy. New Zealand has the Privacy Act 1993 covering privacy concerns relating to New Zealand based Internet businesses. It addresses many of the privacy concerns about e-commerce and gives New Zealand consumers an advantage when they deal with New Zealand-based businesses. The New Zealand Privacy Act 1993, however, does not cover any non New Zealand based Internet businesses. It means that New Zealand consumers have no privacy guarantee if they go to an overseas based web site. Thus, it is necessary to discuss how privacy protection could be achieved in a globally consistent manner. Some possible solutions could be legislation, self-regulation, technological solutions and combination solutions.

7.1 Legislation

Privacy advocates argued legislation is needed to stop the Internet data collection without permission. Other proponents for legislation suggested regulating the privacy concerns by law is better if self-regulation fails to address privacy concerns adequately.

Opponents of privacy legislation argued that compliance cost is a major concern [12]. In fact the creation of legislation does not necessarily generate higher compliance costs than a self-regulatory regime. In the absent of privacy legislation, there might be costs associated with meeting consumer concerns or dealing with privacy risks. There would be sectoral laws combined with voluntary self-regulation and laws relating to confidentiality [12]. All of these would involve compliance costs as well.

Opponents are also concerned that the implementation of a privacy law will be inflexible [12]. The New Zealand Privacy Act shows that legislation can be flexible. Privacy law does not pose an obstacle to the development of e-commerce within New Zealand or for New Zealand business seeking consumer sales overseas [14]. Nevertheless, the New Zealand Privacy Act also shows that legislation may not solve the problems. The New Zealand Privacy Commissioner has an 18 months backlog of complaints to be processed [26]. This indicates that legislation may not be enforceable unless it is properly organised.

7.2 Self-regulation

Web sites must govern themselves if they do not want the government to get involved regarding consumers' privacy concerns. The FTC has expressed a preference for self-regulation in the area of consumer privacy protection due to the fact that technology changes at a rapid pace.

Proponents of self-regulation do not want the government regulating their activities, perhaps fearing an overly bureaucratic system or spiralling compliance costs [14]. They believe that self-regulation could be more flexible. The Online Privacy Alliance was formed in June of 1998 by 50 companies to form a self-regulatory policy for Internet companies [6]. A seal system was selected to promote web sites with fair privacy policies. One established seal program is TrustE. Seals are only given to sites that promote TrustE's three goals for e-commerce and abide by their policies. The three goals are [6]:

- To give online consumers control over their personal information
- Provide web publishers with standardized, cost effective solutions to satisfy businesses and address consumer's anxiety over sharing information
- Provide governmental regulators with evidence that the industry can self regulate.

TrustE is a self-regulatory privacy regime that can build consumers' trust and confidence on the Internet through a program in which web sites can be licensed to display a privacy seal or trustmark on their web sites. Trustmarks provide assurance for consumers that a web site's policy accurately reflects its practices and that there will be a means of recourse if the web site does not abide by its stated policy. It is voluntary for a web site to decide whether it should implement the TrustE privacy regime. It is believed that for those web sites that are willing to regulate themselves can eliminate their consumers privacy concerns.

One reason that the European Union (EU) remains skeptical of the concept of self-regulation is that it does not seem to be working very well in the United States. Despite the moves like IBM's bold declaration that it will not advertise on web sites that do not post privacy policies, Internet businesses have not done a good job of self-regulating privacy [15]. In 1998, FTC expressed a general dissatisfaction with online industry self-regulation efforts [4]. In 1999, although FTC reported that much progress had been made [16], over a third of the sites still did not have a privacy disclosure notice [5]. Of the sites that posted their privacy disclosure, only 13.6 precent were following the FTC's "fair information practices" [5]. The Internet companies should know that if they do not handle privacy concerns in a judicious manner, government regulations will inevitably follow.

7.3 Technological solutions

Some people suggested that the advance of technology could be used as a solution for privacy protection. Some software companies have already developed tools to tackle the privacy concerns. Microsoft and others have released tools and standards to give users more control over their personal information on the web.

One established standard is called Platform for Privacy Preference (P3P). The P3P system works through web browsers to automatically alert users to what information is being collected by a site [5, 27]. The aim of P3P is to have a common privacy language and standard on the web that provides a rich vocabulary for services to express their information practices and for users to express their privacy preferences [12]. Users will be warned and have an option to leave if the site is collecting information for marketing purposes. They can choose to give their personal information only to sites that will not use it for marketing. Thus, P3P technology helps users make informed decisions about when to release their data.

Consumers are not waiting for the government or self-regulation. Some are searching out ways of deleting cookies so they can keep their anonymity. The Anonymizer ensures users surfing the web anonymously, will hide their surfing history when users are browsing the web [17]. It will not stop cookies, but it will allow users to surf the Internet while withholding their IP addresses and other information about them [6]. This ensures that the identity of the users will not be identified.

Recently, a new privacy enhancing cookie management feature has been released for Internet Explorer 5.5 [18, 28]. The version 5.5 of Internet Explorer defaults to allow cookie creation. With version 5.5, users will be asked and prompted in detail before letting a cookie enter into the hard drive. A description of all cookies and their purpose will be given plus a clear distinction between first and third party ones. A default setting will alert the user when a persistent third party cookie is being served or read on the user's machine. A new "Delete all cookies" button is also incorporated. The Internet Explorer 5.5 features prevent cookies being used by advertisers to profile a person and monitor his/her browsing.

Web bug repellents are evolving. Some companies are arming web surfers with tools for finding and repelling web bugs. Personal Sentinal helps surfers to wash the bugs out of the page by alerting consumers to the risk level of any given web site by listing the number of web bugs [19]. Privacy foundation provides a browser plug-in (web bug detector), that allows people to identify the tags and it also corporate web bug tools for e-mail and intranets [21].

It is argued that technical solutions cannot solve the privacy concerns permanently. Although the advance of technology is able to solve the privacy concerns at the moment, it will not work in the near future. Web sites can also utilise advances of technology to obtain personal information as the technology evolves. For example, there might be technology released in the near future that can jump over the technological protection from the user's browser and place a cookie in the user's hard drive. Thus, just using technological solutions is not effective in terms of dealing with the privacy concerns.

7.4 Combination solutions

It is believed that using a combination solution is possible to achieve privacy protection in a globally consistent manner. The combination of legislation, self-regulation and technical solutions may provide synergy that is more effective than a single solution. For example, P3P does not protect data in and of itself. Users must be assured that when they release their data, services will use it only as they have promised. In this case, legislation and self-regulatory regime can help in providing such assurances.

While self-regulation and privacy enhancing technologies are welcome developments in order to enhance privacy protection, they might not be sufficient by themselves and they could be accompanied by legislation.

8. Conclusion

The privacy concerns are posing a barrier to the development of e-commerce. It is an issue that online businesses cannot afford to ignore because privacy concerns are blocking Internet sales. The key is that companies doing businesses on the web need to manage and meet their consumers' expectations where privacy is concerned. A web site with a privacy statement tells consumers that their privacy right is being considered. New Zealand based web sites are not doing very well on this. They should be aware that consumers are looking for privacy protection and a privacy statement can help to ease consumers' concerns.

It would not be good for the business if a client finds that something unexpected has happened to their information, perhaps an unexpected mailing from a different company. Businesses open about their practices and abiding by their privacy statements will win both consumers' confidence and custom. For electronic commerce to succeed, online businesses must build trust with millions of consumers. Respecting consumers' privacy is necessary in order to boost the growth of electronic commerce.

Although consumers have an advantage when they deal with New Zealand based business as privacy concerns are covered by The Privacy Act 1993, global consistency on Internet privacy protection is still necessary. Legislation, self-regulation, technical solutions and combination solutions are different ways that this can be implemented. It is believed that global consistency on Internet privacy protection is important to boost the growth of electronic commerce.

References

[1] Warren, S., and Brandeis, L. (1890). "The Right to Privacy." Harvard Law Review, 4, 193.

[2] Culnan, M. (1993). "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Towards Secondary Information Use." MIS Quarterly, 17(3), 341.

[3] Lim, E. (2000). "Electronic Commerce and the Law". Bcom(Hons) Dissertation, MSIS, University of Auckland.

[4] United States Federal Trade Commission. (1999). Federal Trade Commission online. http: www.ftc.gov.

[5] James, G. (2000). "The price of privacy". Upside. 12(4): 182-190. 2000 Apr.

[6] Cattapan, T. (2000). "Destroying e-commerce's "cookie monster" image". Direct Marketing. 62(12): 20-24+. 2000 Apr.

[7] Anstead, M. (2000). "Taking a tough line on privacy". Marketing. 31. 2000 Apr 13.

[8] Hancock, W. (1997). "Cookies on your hard drive". American Agent & Broker. 69(6): 8-10. 1997 Jun.

[9] Federal Trade Commission, Privacy Online: A Report to Congress, at 3 & n.1 l (June 1998), available in http://www.ftc.gov/reports/privacy3/priv-23a.pdf (citing Business Week/ Harris Poll: Online Insecurity, Bus. Wx., Mar. 16, 1998, at 102).

[10] Krauss, M. (2000). "Don't kid yourself--consumers do pay attention to privacy". Marketing News. 34(5): 13. 2000 Feb 28.

[11] Paynter, J. and Pearson. M. (1998). "An analysis of WWW-based Information Systems" In Chow, W.S. (ed) *Multimedia Information Systems in Practice*, Springer, Singapore, 1998, pp 53-63.

[12] Slane, B (2000). "Killing the Goose? Information Privacy Issues on the Web." http://www.privacy.org.nz/media/Killgoos.html.

[13] Ministry of Economic Development. (2000). "New Zealand's Privacy Act and Electronic Commerce". http://www.ecommerce.govt.nz/privacy/index.html.

[14] Slane, B (1999). "Privacy Protection: A Key to Electronic Commerce." http://www. Privacy.org.nz/people/apec.html.

[15] Gillin, P. (1999). "Privacy politics". Computerworld. 33(18): 30. 1999 May 3.

[16] FTC, Self-Regulation and Privacy Online: A Report to Congress, at 6 (July 1999), available in http://www.ftc.gov/os/1999/9907/privacy99.pdf.

[17] The Anonymizer. (2000). http://www.anonymizer.com.

[18] The New Zealand Herald. (2000). “Virtual cookies can be either good or bad”. The New Zealand Herald, Sep 12, 2000.

[19] Stefanie, O. (2001). “Reversal of fortune – tracking web trackers”. ZD Net News, Mar 5, 2001. http://www.zdnet.com/zdnn/stories/news/0,4586,2692472,00.html

[20] Satitkit, S. (2001). “User Perceptions of Web site Design in the Travel Industry: an Evaluation Model”, unpublished, MCom project , University of Auckland.

[21] Privacy Foundation (2001) “Web Bugs” http://www.privacyfoundation.org/resources/webbug.asp

[22] Anderton, J. (2001). "NZ web retailers not all user friendly". Media Statement, released 19 Mar

[23] Ministry of Economic Development (2001). E-commerce: A guide for New Zealand Business. p 28-29.

[24] TrustE (2001). http://www.truste.org

[25] Roy Morgan Research. (2001). “Privacy and the Community, July 2001”. Office of the Federal Privacy Commissioner. http://www.privacy.gov.au/publications/rcommunity.html

[26] The New Zealand Herald. (2001). “Protecting privacy is their business” http://www.nzherald.co.nz/storydisplay.cfm?thesection=news&thesubsection=&storyID=184614&reportID=58554

[27] Platform for Privacy Preferences. (2001). http://www.w3.org/P3P/

[28] Microsoft. (2001). http://www.microsoft.com