
Connection to www
ard and Payment Information
opping at Amazon.com is safe.
uldn't have it any other way. In
ve back every credit card
ase with our Amazon.com Safe
pping Guarantee.
guarantee that every transaction
make at Amazon.com will be safe.
s means you pay nothing if
authorized charges are made to
ur card as a result of shopping at
mazon.com. See guarantee details
elow.

A snoop at privacy issues on the internet in New Zealand

By Winnie Chung

The internet is an amazing tool. 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 around the world. But the internet also allows for the efficient and inexpensive collection of vast amounts of information. If internet users are not careful, they can unintentionally give away information about themselves. The prevalence, ease and relative low cost of such information collection distinguishes the online environment from more traditional means of commerce and information collection. This raises consumer concerns about threats to their personal privacy while online.

Consumers worry about the safeguarding of their personal information after it has been collected and fear that the information may be misused

The privacy issues on the web need to be considered. The internet is international and largely unregulated. This means the laws of any one country do not usually apply to internet activities originating in other countries. Thus it is necessary to consider how privacy protection could be achieved in a globally consistent manner.

In this paper, the following section gives a general explanation of internet privacy and outlines the concerns. Subsequent sections deal with arguments against internet privacy; arguments for internet privacy; New Zealand privacy law; how internet privacy is being addressed in overseas and New Zealand websites; results of user surveys on the banking and travel sector; and the importance of addressing internet privacy globally, along with some solutions.

INTERNET PRIVACY

Warren and Brandeis (1890) defined privacy as the "right to be let alone". Westin (1967) said it is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Privacy can be divided into four basic categories: information privacy, bodily privacy, communications privacy and territorial privacy (Davis, 1996). When dealing with internet privacy, the concern is with information privacy (Zimmerman, 2001). Information privacy exists when the usage, release and circulation of personal information can be controlled (Culnan, 1993). Invasions of privacy occur when individuals cannot maintain a substantial degree of control over their personal information and its usage (Lim, 2000).

The internet has a vast potential for privacy violation as technological innovations have become more advanced (Zimmerman, 2001). It allows for the efficient, inexpensive collection of information without consumer consents. It can track consumers in unique ways, whether or not a consumer is aware of it. This includes consumer preferences, interests and even credit card information.

In 1999, a United States Federal Trade Commission study (Federal Trade Commission, 1999) discovered that 92.8 per cent of websites were gathering at least one type of identifying information (name, e-mail address, postal address), while 56.8 per cent were collecting at least one type of demographic information (gender and preferences). This information has real value in the information economy, especially when combined with other data (Cate, 2000). The monetary value of this information explains why so many websites gather personal information. This raises consumer concerns about privacy rights. Consumers worry about the safeguarding of their personal information after it has been collected and fear that the information may be misused.

What are the concerns?

Internet users are concerned that:

- Visits to websites 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 information will be stolen.

The advances in internet and database technology increase concerns about information privacy. Data entered into forms or contained in existing databases can be combined almost effortlessly with transaction records and records of an individual's every

mouse-click on the internet. Privacy concerns further increase as data-mining tools and services become more widely available.

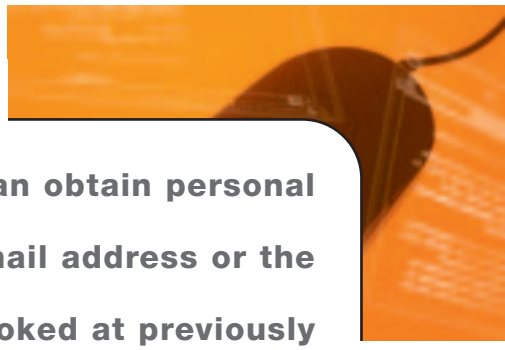
Cookies are widely used to identify users of a website and some users consider this an invasion of their privacy. Users are prompted for information such as gender, age, buying preferences or even e-mail address. For example, if you go online to buy a book from Amazon.com, you will be prompted to enter your e-mail address, billing address and other details. This information will be packaged into a cookie and sent to the user's hard drive, which stores it for later user identification. When the user revisits the same website, the user's browser will send the cookie to the web server. By recognising the information in the cookie, the web server recognises the user and a customised web page could be generated according to the interests and preferences of the user. Information about one's movements in a website can also be stored in a cookie. The main concern is that all this is done without the user's knowledge (Zimmerman, 2001).

The situation is made worse if the cookies are generated through banner advertisements from direct marketing companies. Most websites have limited capability to read cookies from a user's hard drive that the website itself sent on a previous visit. But a direct marketing company can post banner advertisements on hundreds of different websites and send its own cookies in addition to the cookie sent from the website itself. This means direct marketing companies have the added capacity to read the cookies sent by banner advertisements situated on different websites as long as the same direct marketing company owns both banners (Zimmerman, 2001).

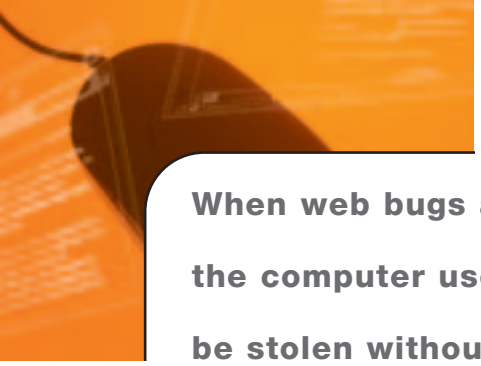
By using cookies, businesses can obtain personal information such as buying habits, e-mail address or the portions of a website that were looked at previously. This information can be combined into mailing lists for direct marketing purposes or even be on-sold to third parties. For example, America Online shares information about its users with various partners including companies that do direct mailing and telephone solicitations (James, 2000).

A web bug, utilising online tracking technology, is another widely used instrument that poses a privacy threat. Web bugs are invisible pieces of code that can be used for several purposes ranging from secretly tracking a user's web travels to pilfering computer files (Stefanie, 2001). The simplest form of web bug is a small graphic interchange format that works with cookies to send information to third parties about a visitor's online travels. An executable bug can install a file on hard drives that collects information whenever users are online. A script-based executable bug can be installed on a user's computer and then take any document from the computer without notice. Another form of script-based executable bug is based on servers. It can track a visitor's travels on the web and control that person's computer from its server. It can launch multiple browser windows when a visitor tries to exit a site.

Many websites and internet advertising companies place web bugs on their pages to collect information such as what pages are being read most often. As mentioned earlier,



By using cookies, businesses can obtain personal information such as buying habits, e-mail address or the portions of a website that were looked at previously



When web bugs are used maliciously or nefariously, the computer user's entire e-mail address book can be stolen without notice

the bugs can be used in more invasive ways such as to capture a visitor's internet protocol address or install pernicious files in the visitor's hard drive.

The concern is that with a web bug, the visitor's computer can be exposed to malicious sites that can take any files or information from programs on the visitor's hard drive without his or her knowledge and consent. A report shows that 16 million out of 51 million pages that were scanned contained at least one web bug that had been attached by a third party, such as an advertising network (Stefanie, 2001). When web bugs are used maliciously or nefariously, 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 a list of catalogue purchasers' names and addresses (Cattapan, 2000). This allows cross-referencing that matches information with real-world names, addresses and histories of offline mail order purchases (Anstead, 2000). The acquired names and addresses can be linked with the cookies so DoubleClick not only knew where people were online, but who they were, where they live and their phone numbers. This should be the most comprehensive customer database in the world that can be used for direct marketing purposes.

The security of credit card information for online purchases is another of the privacy concerns. The internet creates a potential for fraudulent activities, as few regulatory standards exist (Hancock, 1997). Bibliofind, a subsidiary of Amazon.com, admitted that hackers, undetected over four months, stole 98,000 credit card numbers. It is not hard to find a website that publishes a list of credit card numbers and other related information. The card numbers can be easily downloaded by anyone. The concern is that even though consumers permit a website to collect their personal information, they may still fear that the information could be disclosed to undesirable people due to lack of security on the web server.

ARGUMENTS AGAINST INTERNET PRIVACY CONCERNS

Some argue that internet privacy concerns are nothing special; that people are just over-sensitive as they realise how fast the internet is growing; that shopping online is no different to in-store shopping in terms of tracking customer behaviour. Tracking a person's online navigation can be compared to a security camera watching customers as they move around in a store. Most people think it is normal for a store to use cameras to track the movement of customers, even though it can allow customers' identification. If customers don't think this is a concern, then they should have the same attitude to being tracked via the internet when browsing a website.

And although cookies can be used to identify visitors to a website, in fact they cannot find out names, addresses and other personal information unless visitors have provided such information voluntarily (Cattapan, 2000). Thus the use of cookies is not a main point regarding privacy concerns. In fact, some people are willing to give away their personal information in return for discounts and other benefits (Roy Morgan Research, 2001). The use of cookies for online purchases is no different to mail order catalogue purchases 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 the point that internet privacy concerns could be trivial. Consumers do not want to reveal their information online for marketing purposes, but consumer information can easily be found in telephone books or other sources and this information can be used by marketers, who can send flyers to physical letterboxes based on the information. It is argued that getting rid of online junk mail is easier than getting rid of actual junk mail. Thus privacy concerns regarding online junk mail are considered to be trivial.

In addition, some websites collect personal information but never use it. For example, Steinlager is a New Zealand website that offers competitions to visitors who have to provide their personal information in order to join the competition. It is mentioned on the website that information obtained will be used for marketing purposes. This site was studied as part of another project (Paynter and Pearson, 1998), but the visitor information so far has not been used for any form of direct marketing. Thus it is not really a privacy concern when obtained information is not being used.

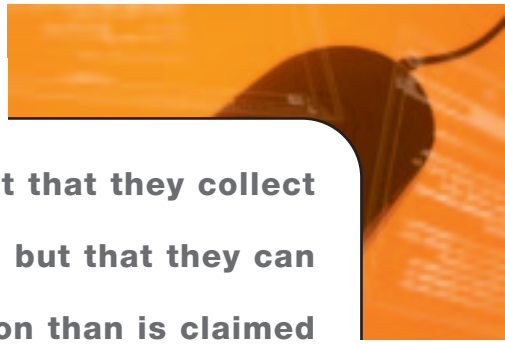
ARGUMENTS FOR INTERNET PRIVACY

The previous section may provide several arguments that suggest internet privacy concerns are not a special worry, but website owners should still consider this issue.

It is understandable that customers have more privacy concerns when they shop online compared to in-store shopping. Store cameras are usually perceived as security tools to help prevent shoplifting and they are generally acceptable to most customers. In addition, cameras do not always allow the identification of a particular customer. This is different to tracking consumers online, where identification of a particular website visitor is easier.

Mail order catalogue purchases allow marketers to track consumers' buying histories only. Cookies, however, can associate names and addresses with other information (provided voluntarily by the website visitor). The fear about cookies is not that they collect information about consumers, but that they can collect much more information than is claimed.

Surveys show that the primary reason most non-internet users avoid the internet is because of concerns about the privacy and safety of their personal information and communications (Federal Trade Commission, 1998). Privacy concerns prevent some consumers from buying products on the web. A 1999 study by marketing research firm NFO Interactive found that almost three out of four consumers who browse the internet never make a purchase online (James, 2000). Those consumers said they would be more likely to buy if they could be assured that their privacy would be respected. A recent study also suggests that privacy is one of the concerns that stop people in Malaysia from making purchases via the internet (Lim and Paynter, 2001). A telephone survey of 750 New



The fear about cookies is not that they collect information about consumers, but that they can collect much more information than is claimed

Since businesses are developing relationships with consumers, it helps if consumers know that businesses care about them

Zealanders found that 86 per cent of respondents were concerned (including 76 per cent who were very concerned) if a business monitors the activities of consumers on the internet, recording information on the sites they visit, without the consumers' knowledge (UMR Research Ltd, 2001).

Internet-based businesses should care about such privacy concerns because consumers care about the issue. Since businesses are developing relationships with consumers, it helps if consumers know that businesses care about them. Surveys show that people care if they see a privacy statement and they also care if a privacy statement has been approved by a third party, such as TrustE (Krauss, 2000). To boost the development of e-commerce, information privacy concerns should be treated seriously as they are discouraging consumers from using the internet to buy goods and services.

NEW ZEALAND PRIVACY LAW

Privacy Act 1993

New Zealand's Privacy Act 1993 does not create a right of privacy, nor is its recognition of privacy interests absolute (Slane, 2000). Its coverage includes both electronic and paper information. Any business based in New Zealand and wishing to engage in electronic commerce with consumers must ensure that its activities comply with the Privacy Act, to the extent that the activities involve personal information about the 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 (Slane, 2000). The Privacy Act applies to the handling of all personal information collected or held by agencies, whether in the public or private sectors.

In New Zealand, consumer privacy concerns can largely be met through businesses complying with the Privacy Act. Information Privacy Principles 3 and 5 of Section 6 of the Privacy Act 1993 are closely related to New Zealand websites. Principle 3 sets out how an agency should go about collecting information from someone. Agencies are required to alert people to a number of matters when information is collected from them (Office of Privacy Commissioner, 2002). The matters include:

- The fact of collection.
- The purpose of collection.
- Intended recipients of the information.
- Contact details for the agency collecting and the agency 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.

Principle 5 is related to the storage and security of personal information. It sets out how an agency should go about holding personal information (Office of Privacy Commissioner, 2002). Agencies are required to ensure that:

- The information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:
- Loss.
- Access, use, modification or disclosure, except with the authority of the agency that holds the information.
- Other misuse.
- If it is necessary for the information to be given to a person in connection with the provision of

a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

The Privacy Act emphasises the use of civil law in dealing with complaints (Office of Privacy Commissioner, 1999a). It does not establish a statutory tort of invasion of privacy and people cannot sue in the courts. Instead, complaints are filtered by an ombudsman-like process and the Act allows recourse to civil remedies through a tribunal only after the Privacy Commissioner has decided to take the investigation no further (Office of Privacy Commissioner, 1999b).

Tort of invasion of privacy

Besides the Privacy Act 1993, New Zealand law includes the tort of invasion of privacy. "Prior to the enactment of the Privacy Act in New Zealand, there were only scattered rules of law and statutory provisions that dealt with particular aspects of privacy. At common law, the existence of a right to privacy enforceable by a cause of action in tort for invasion of privacy has only recently been accepted in New Zealand, but it has never been applied to the particular facts in question" (Roth, 1998). The tort of invasion of privacy has broader coverage and more remedies than the Privacy Act 1993. Four factors need to be proven for a tort of invasion of privacy (Eagles, Longdin, Grantham, Prasad, Rickett, Cripps, Mapp, Gunasekara and Brown, 2001):

- Whether the disclosure of private facts is a public disclosure.
- Whether the facts made public are private facts and not in the public domain.
- Whether the information made public is highly offensive and objectionable to a reasonable person with ordinary sensibilities.
- The nature and extent of legitimate public interest in having the matter made public.

If one's privacy is being invaded and the above factors are proven, one can bring a common law action and sue for damages. An example of a common law remedy based on the tort of invasion of privacy is an interim injunction. New Zealand websites should recognise that if personal information is collected and published without consent, they may be held liable under the tort of invasion of privacy, providing the above four factors are proven. From a practical point of view, however, it is unlikely a user would issue proceedings for a breach of invasion of privacy that has occurred through a website because it would be too expensive and time-consuming to take it to court.

ADDRESSING PRIVACY ON OVERSEAS AND NEW ZEALAND WEBSITES

A privacy policy statement that provides consumers with more control will reduce consumer concerns (Cattapan, 2000). To comply with Information Privacy Principle 3, New Zealand websites 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

The Privacy Act emphasises the use of civil law in dealing with complaints. It does not establish a statutory tort of invasion of privacy and people cannot sue in the courts

A mention in the privacy statement about the security and storage of collected personal information can help eliminate concerns about credit card theft

of that information (Ministry of Economic Development, 2000). Thus, matters can be drawn to people's attention before the information is collected. Complying with Principle 5 would add to consumers' confidence. A mention in the privacy statement about the security and storage of collected personal information can help eliminate concerns about credit card theft due to unsafe storage by the agencies. Compliance with Principles 3 and 5 can help build trust between businesses and consumers.

Addressing privacy on overseas websites

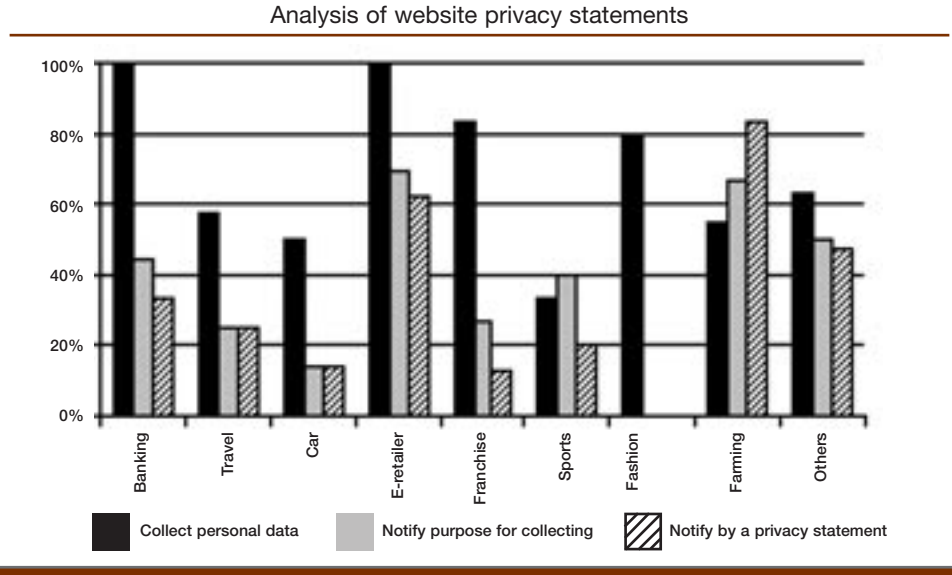
Slane (1999) mentioned the results of surveys conducted in Hong Kong and United States in 1998. The Privacy Commissioner for Personal Data in Hong Kong conducted a survey of websites. The results indicated that although 63.8 per cent of the websites surveyed provided forms to collect personal data, only 31.9 per cent had statements notifying people of the purposes for collecting the data. Only six per cent had a privacy policy statement. By 1999, the result had improved, but there was still some way to go; 77 per cent of websites notified people of the purposes for collecting the information and 23 per cent had a privacy policy statement. In 1998, the Federal Trade Commission examined the practices of 1400 commercial sites on the web. Although 85 per cent of the sites surveyed collected personal information from consumers, only 14 per cent provided any notice about the purpose of collection and only two per cent provided a comprehensive privacy policy. The above results show that personal information is being collected from websites, most of which do not have a comprehensive privacy policy.

Addressing privacy on New Zealand websites

New Zealand consumers have the same rights irrespective of whether the transaction is carried out electronically or by traditional means (Ministry of Economic Development, 2001). Many New Zealand web retailers are not providing enough information to safeguard consumer rights (Anderton, 2001). New Zealand-based businesses should be warned that privacy concerns need to be treated seriously. In New Zealand, website privacy statements are expected under Information Privacy Principle 3 (Ministry of Economic Development 2001). No published survey has been conducted to ascertain the level of compliance with Principle 3 by New Zealand-based websites (Slane, 1999).

For this article, 140 New Zealand-based websites were chosen to evaluate how privacy issues are being handled by these sites. The 140 websites were chosen as the best-known ones from nine different sectors: banking, travel, car, e-retailer, franchise, sports, fashion, farming and others. A coding sheet was used to record the presence or absence of attributes for each website. The coding sheet recorded three attributes for each website: (i) whether it collects any personal data in any form including cookies; (ii) whether it notifies people about the purpose for collecting the data; and (iii) whether it notifies people by a privacy policy statement. Some websites were so large and disparate in nature (e.g. 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 a site might have a privacy statement, but the statement would be lacking from the overall site. Where the presence or absence of a privacy statement could not be easily ascertained, then the site is

FIGURE 1



not included in the study. **Figure 1** shows the results for different sectors.

All websites in the banking sector collected personal data, 44 per cent of websites provided notice of the collection purpose and 33 per cent had a privacy policy. Fifty-seven per cent and 50 per cent of the sites from the travel and the car sectors respectively collected personal data. Only 25 per cent and 14 per cent of travel and car sites respectively provided notice of the collection purpose and those provided privacy statements as well. All e-retailer sites collected personal data and of those, 69 per cent notified the purpose of collection and 62 per cent notified by way of a privacy statement. For the franchise sector, 83 per cent of sites collected personal data, but only 27 per cent provided notice of the collection purpose and only 17 per cent notified by a privacy statement. Thirty-three per cent and 80 per cent collect personal data in the sports and fashion sectors respectively. Forty per cent from the sports sector notified purpose of collection and 20 per cent provided a privacy statement. However, the fashion sector sites had not made any notification regarding information collection.

It is interesting to note that in the sports sector, the percentage that notifies the collection purpose (40 per cent) is more than the percentage that collects personal data (33 per cent). The reason is because some websites in the sports sector claim they collect personal data when, in fact, they do not. The same phenomenon appears in the farming sector. Only 55 per cent of farming sites collect personal data, but 67 per cent notify the purpose of collection and 83 per cent provide a privacy statement. This implies that the websites of some sectors are more likely to consider the issue of privacy. However, they are not seriously dealing with this issue. They notify the purpose of collection in order to protect themselves. This type of website tends to use a standard policy or statement from third parties without really considering whether it applies to its site or not.

The results in Figure 1 indicate that websites in different sectors are not uniform in respecting consumer privacy by providing notification of the purpose of collection. For instance, it is interesting that although a large proportion of sites in the fashion sector collect personal data, no notice is given regarding information collection. This is the sector that tends to ignore the issue of privacy completely. In contrast, for the travel and car sectors, those sites that notified the purpose of collection tend to provide a privacy policy. If sites consider privacy concerns, they will have an explicit privacy policy rather than just notifying people without any comprehensive privacy statement.

Some New Zealand websites consider privacy concerns and show they treat the issue seriously. Further improvement is necessary, however

It seems that some sectors such as banking and e-retailing tend to consider the issue more than others, so they are more likely to provide a privacy statement. This could be explained by the fact that banking and e-retailer websites are transaction-oriented, hence more personal information is involved. The websites represented for other sectors, such as fashion and franchise, either ignore the issue of privacy or they simply do not have this idea in mind as part of their website design and/or operation.

In general, 66 per cent of the 140 websites studied collected some sort of personal data from consumers. Among those that collected personal information, 29 per cent notified the purpose of collection and 25 per cent 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 four per cent. This implies that most websites that addressed privacy concerns tend to notify people about the purpose of collecting personal information with a privacy statement. Otherwise, websites simply ignored consumer privacy.

The results indicate that New Zealand-based websites collect personal data in much the same way as overseas websites do. Some New Zealand websites consider privacy concerns and show they treat the issue seriously. Further improvement is necessary, however, if New Zealand websites want to ease consumer privacy concerns.

In a later study (Fung, 2001), 20 medical-related New Zealand websites were chosen from the electronic Yellow Pages (www.yellowpages.co.nz) and examined for the purpose of this paper. Only unique sites were examined. That is, those with multiple listings or branches were ignored. Those with only a simple banner in the electronic Yellow Pages were also excluded. Of the 20 chosen websites, three were medical insurance companies, or offered a medical insurance policy as one of their services; one was for health professionals to use to support travelling patients; and the rest were medical clinics and hospitals. The results show that 19 collected personal information, but only one had a privacy statement and it was very obscure; three used cookies; and none mentioned the purpose for which the information was collected. Information Privacy Principle 3 requires that a well-expressed website should have a privacy statement. The websites studied all failed to meet such a requirement.

User surveys on the banking and travel sector in New Zealand

The previous section suggests that privacy issues are more likely to be related to transaction-oriented sectors. Two sectors were selected to draw user responses in order to understand the customer perspective. These sectors were selected because both are transaction-orientated, but one (banking) is believed to address the privacy issue more than the other (travel).

Questionnaires were given to customers in the two sectors using a convenience sampling of staff and Stage 3 or above students in the Management Science and Information System department of The University of Auckland. Samples of 200 and 130 were targeted in the banking and travel sectors respectively. Of these, 184 and 101 were usable in the banking and travel sectors respectively. The surveys found that customers from both sectors have concerns regarding privacy. It is one of the main factors preventing them from using internet banking and making travel bookings via the internet. Results also indicate that customers in the travel sector have more privacy concerns than those in

the banking sector. This could be explained by the fact that more personal information is involved in the travel sector and the banking sector has a longer history of maintaining privacy. Online travel transactions tend to require the customer to provide much more personal information. In the banking sector, however, customers give less information, although cookies may be collected by websites. The surveys are reported in more detail in Satitkit (2001) and Chung and Paynter (2002).

In general, the surveys confirm that privacy concerns constrain the use of internet for online transactions. Websites need to understand that they have to show customers that they respect their privacy. The results also reveal that even when a website provides a comprehensive privacy statement, some customers still do not perceive that they are safe in terms of privacy maintenance. It could be because some websites provide only a standard privacy statement, leading customers to think that these websites do not seriously respect their privacy rights. This suggests that a website not only needs to provide a comprehensive privacy statement, it should also have a privacy statement that customers can see is tailored specifically for the website and the information and issues pertaining to it.

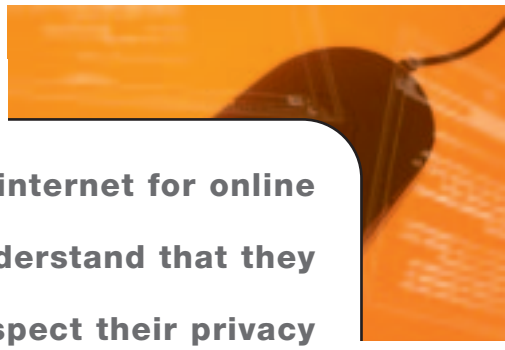
MECHANISMS FOR ADDRESSING GLOBAL PRIVACY ISSUES ON THE INTERNET

It must be noted that the internet is internationally unregulated. This means the laws of any one country do not usually apply to internet activities originating in other countries. Privacy needs to be protected across borders because of the flow of information between countries.

The 1995 European Data Protection Directive regulates the protection of privacy for the transmission of personal information between countries. It protects the rights of individuals regarding the use of information about them (Freshfields Bruckhaus Deringer, 2000). It also imposes an obligation on member states to ensure that the personal information of European citizens is covered by law when that information is exported to, and processed in, non-European Union countries (Gips, 1999). New Zealand businesses with a European website should adhere to the directive if they are collecting personal information from consumers. This law also governs the transmission of personal information from an office in EU countries to the office in New Zealand.

The United States doesn't have generally applicable data protection laws (Freshfields Bruckhaus Deringer, 2000). Since the European Data Protection Directive provides that personal information may be sent only to countries that ensure an adequate level of protection on personal data, the US fears that personal information transferred from EU countries may be blocked. In 2000, the EU and US agreed on the safe harbour principle allowing the transfer of personal information from the EU to the US (Freshfields Bruckhaus Deringer, 2000). US companies have to sign the Safe Harbour Principles in order to receive personal information from the EU.

New Zealand has the Privacy Act 1993 covering privacy concerns relating to New



Privacy concerns constrain the use of internet for online transactions. Websites need to understand that they have to show customers that they respect their privacy

New Zealand consumers have no privacy guarantees if they go to an overseas-based website, especially those from countries that have undeveloped privacy legislation

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. But the Act does not cover any non-New Zealand-based internet businesses. It means that New Zealand consumers have no privacy guarantees if they go to an overseas-based website, especially those from countries that have undeveloped privacy legislation. Thus it is necessary to discuss how privacy protection could be achieved in a consistent manner globally. The use of legislation, self-regulation, technological solutions and a combination of solutions are some of the possible ways to achieve this.

Legislation

Privacy advocates argue that legislation is needed as it can constrain the capturing of internet data without user permission. Other proponents for legislation suggest that regulating privacy concerns by law is better if self-regulation fails to address privacy concerns adequately.

Opponents of privacy legislation argued, however, that compliance cost is a major concern (Slane, 2000). In fact, the creation of legislation does not necessarily generate higher compliance costs than a self-regulatory regime. In the absence 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 (Slane, 1999). All of these would involve compliance costs as well.

Opponents are also concerned that a privacy law might be inflexible. 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 businesses seeking consumer sales overseas (Slane, 1999). However, the Privacy Commissioner does not have sufficient resources to enforce the law. As at 1999, the queue of the unallocated complaints was 14 months long (Office of Privacy Commissioner, 1999a).

Self-regulation

Websites must govern themselves if they do not want the government to get involved regarding consumer privacy concerns. The Federal Trade Commission had 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 (Slane, 1999). They believe that self-regulation could be more flexible. The Online Privacy Alliance was formed in June, 1998, by 50 US companies to produce a self-regulatory policy for internet companies (Cattapan, 2000). A seal system was selected to promote websites with fair privacy policies. One established seal program is TrustE. Seals are given only to sites that promote TrustE's three goals for e-commerce and abide by their policies. The three goals are:

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

TrustE is a self-regulatory privacy regime that can build consumer trust and confidence on the

internet through a program in which websites can be licensed to display a privacy seal or trustmark on their sites. Trustmarks provide assurance for consumers that a website's policy accurately reflects its practices and that a means of recourse is available if the site does not abide by its stated policy.

One reason that the EU remains sceptical about the concept of self-regulation is that it does not seem to be working very well in the US. Despite moves like IBM's bold declaration that it will not advertise on websites that do not post privacy policies, internet businesses have not done a good job of self-regulating privacy (Gillin, 1999). In 1998, the FTC expressed a general dissatisfaction with online industry self-regulation efforts (Federal Trade Commission, 1999). Although the FTC reported in 1999 that much progress had been made, more than one-third of sites still did not have a privacy disclosure notice (James, 2000). Of the sites that posted their privacy disclosure, only 13.6 per cent were following the FTC's "fair information practices". Internet companies should know that if they do not handle privacy concerns in a judicious manner, government regulation will inevitably follow.

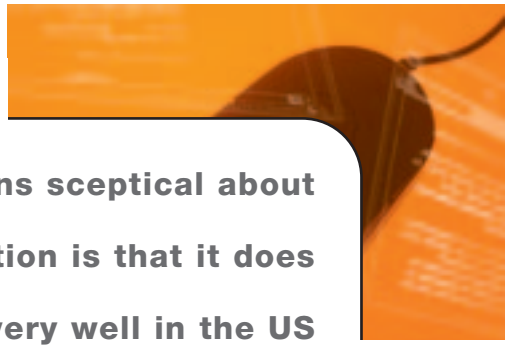
Technological solutions

Some people suggest that the advance of technology could be used as a solution for privacy protection (Lim, 2000). Some software companies have already developed tools to tackle 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). P3P works through web browsers to automatically alert users to what information is being collected by a site (James, 2000). The aim of P3P is to have a common privacy language (e.g. Extensible Mark-up Language) and web standards that provide a rich vocabulary for sites to express their information practices and for users to express their privacy preferences (Slane, 2000). 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 purposes. 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 program ensures users' anonymity when using the web by hiding their surfing history (The Anonymizer, 2000). It will not stop cookies, but it will allow users to surf the internet while withholding their IP addresses and other information about themselves (Cattapan, 2000). This ensures that users will not be identified.

New privacy-enhancing cookie management features have been recently released for Internet Explorer. Previous Internet Explorer versions default to allow cookie creation. With newer versions (e.g. 5.5), users will be asked and prompted in detail before letting a cookie enter their hard drive. A description of all cookies and their purpose will be given, plus a clear distinction between first- and third-party



One reason that the EU remains sceptical about the concept of self-regulation is that it does not seem to be working very well in the US

cookies. 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 newer versions of Internet Explorer prevent cookies being used by advertisers to profile a person and monitor his/her browsing.

Web bug repellents are also evolving. Some companies are arming web surfers with tools for finding and repelling web bugs. Personal Sentinel helps surfers to wash the bugs out of the page by alerting them to the risk level of any given website by listing the number of web bugs (Stefanie, 2001). Privacy Foundation provides a browser plug-in (web bug detector) that allows users to identify the tags and incorporates debug tools for e-mail and intranets (Privacy Foundation, 2001).

It is argued that technological solutions cannot solve the privacy concerns permanently. Although the advance of technology is able to solve concerns at the moment, it will not work in the near future. Websites can also utilise the advances of technology to obtain personal information as the technology evolves. For example, technology may be 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 in the long term.

Combination solutions

It is suggested that by using a combination solution, it is possible to achieve privacy protection in a globally consistent manner (Lim, 2000). 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, websites will use it only as they have promised. In this case, legislation and a 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.

CONCLUSION

Privacy concerns are posing a barrier to the development of e-commerce, especially to websites that are transaction-oriented. It is an issue that online businesses cannot afford to ignore because privacy concerns are blocking internet sales. The key is that companies doing business on the web need to meet their consumers' expectations where privacy is concerned. It is important to have a website with a privacy statement that tells consumers their privacy rights are being considered carefully. New Zealand-based websites are not doing very well on this count. They should be aware that consumers are looking for privacy protection and a comprehensive privacy statement can help to ease consumer concerns.

It would not be good for a 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 consumer confidence and custom. For electronic commerce to succeed, online businesses must build trust with millions of consumers by respecting their privacy rights.

Winnie Chung
POST GRADUATE STUDENT
Department of Management Science and Information Systems
The University of Auckland Business School
E-mail: winniec@ihug.co.nz

Although consumers have an advantage when they deal with New Zealand-based businesses as privacy concerns are covered by the Privacy Act 1993 and the tort of invasion of privacy, 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. Global consistency on internet privacy protection is important to boost the global growth of electronic commerce.

KEY SOURCES AND FUTURE READINGS

Office of the Privacy Commissioner — http://www.privacy.org.nz/top.html

Ministry of Economic Development — http://www.ecommerce.govt.nz/privacy/index.html

OECD — http://www.oecd.org

REFERENCES

Anstead, M. (2000). Taking a tough line on privacy. *Marketing,* 31, Apr 13.

Anderton, J. (2001). NZ web retailers not all user friendly. Media statement, Mar 19.

Cate, F.H. (2000). Principles of Internet Privacy. *Connecticut Law Review,* 32, pp 877-896.

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

Chung, W., & Paynter, J. (2002). An evaluation of Internet Banking in New Zealand. Proceedings of the 35th Hawaii International Conference on System Sciences, Hawaii, Jan, p 185.

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

Davies, S. (1996). *Big Brother: Britain's web of surveillance and the new technological order,* Pan, London, p 23.

Eagles, I., Longdin, L., Grantham, R., Prasad, M., Rickett, C., Cripps, C., Mapp, W., Gunasekara, G., & Brown, L. (2001). *Law in Business & Government in New Zealand,* 3rd Edition, Palatine Press, Auckland.

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

Federal Trade Commission (1999). Self-Regulation and Privacy Online: A Report to Congress, Jul. http://www.ftc.gov/os/1999/9907/privacy99.pdf

Freshfields Bruckhaus Deringer (2000). Data Protection European Commission agrees to US safe harbour principles. Aug. http://www.freshfields.com/practice/ipit/publications/22367.pdf

Fung, M. (2001). The Impact of Information Technology in Healthcare Privacy. Department of Management Science and Information Systems Working Paper, No.235, The University of Auckland Business School.

Gillin, P. (1999). Privacy politics. *Computerworld,* 33(18), p 30, May 3.

Gips, M. (1999). Privacy Privation. *Security Management,* 43(1), p 16.

Hancock, W. (1997). Cookies on your hard drive. *American Agent & Broker,* 69(6): pp 8-10, Jun. http://www.privacy.org.nz/people/apec.html

James, G. (2000). The price of privacy. *Upside,* 12(4), pp 182-190, Apr.

Krauss, M. (2000). Don't kid yourself — consumers do pay attention to privacy. *Marketing News,* 34(5), p 13, Feb 28.

Lim, E. (2000). Electronic Commerce and the Law. Unpublished BCom(Hons) dissertation, Department of Management Science and Information Systems, The University of Auckland.

Lim, L.H., & Paynter, J. (2001). Malaysia B2C. *Malaysian Journal of Library & Information Science.* 5(2), Dec.

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

Ministry of Economic Development (2001). *E-commerce: A guide for New Zealand Business.* pp 28-29.

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

Privacy Foundation (2001). Web Bugs. http://www.privacyfoundation.org/resources/Webbug.asp

Roth, P. (1998). Privacy Law & Practice, Butterworth, Wellington.

Roy Morgan Research (2001). Privacy and the Community, Jul. Office of the Federal Privacy Commissioner. http://www.privacy.gov.au/publications/rcommunity.html

Satitkit, S. (2001). User Perceptions of Website Design in the Travel Industry: an Evaluation Model. Unpublished MCom project, The University of Auckland.

Slane, B. (1999). Privacy Protection: A Key to Electronic Commerce. The Office of the Privacy Commissioner. http://www.privacy.org.nz/people/apec.html

Slane, B. (2000). Killing the Goose? Information Privacy Issues on the Web. The Office of the Privacy Commissioner. http://www.privacy.org.nz/media/Killgoos.html

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

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

The Office of Privacy Commissioner (1999a). Adequacy of data protection measures: the New Zealand case. Speech by Blair Stewart, Assistant Privacy Commissioner, 12th Privacy Laws and Business Annual International Conference, "New Data Protection Law, Issues, Solutions, Action", Cambridge, UK, Jun 29. http://www.privacy.org.nz/media/adequacy.html

The Office of Privacy Commissioner (1999b). Privacy protection: A Key To Electronic Commerce. Address by Privacy Commissioner, Bruce Slane, New Zealand Law Conference, Rotorua, Apr 9. http://www.privacy.org.nz/media/mediatop.html

The Office of the Privacy Commissioner (2002). Information Privacy Principles. http://www.privacy.org.nz/people/fact3-0.html

UMR Research Ltd (2001). A Summary Report on Individual Privacy in New Zealand by the Privacy Commissioner. Sep. http://www.privacy.org.nz/recept/Final%20Rpt%20OmniResults-September011.pdf

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review,* 4, p 193.

Westin, A.F. (1967). *Privacy and Freedom,* Atheneum, New York, p 7.

Zimmerman, R.K. (2001). The way the cookies crumble: internet privacy and data protection in the twenty-first century. *New York University Journal of Legislation and Public Policy,* 4, 2000-2001.