ABSTRACT

In this era of Internet, Information Privacy has become a very important issue. The kind and amount of information that is collected from a user and the way in which the company is using this information has become an issue with ethical, moral and technological overtones. This report aims to look at the issues regarding information privacy in the context of Internet from the user's point of view. It looks at the different kinds of information collected, how it is collected, what happens to it, who (mis) uses it and how end users can control the information flow as well as what the companies and agencies are doing to ensure safety of customer information. This study does not restrict itself to Internet based transactions, but rather looks into the issues as wide as those related to online medical records, government and employer initiated monitoring. The report also presents the result of a privacy survey conducted on Singapore based websites, which shows that on the whole, Singaporean sites are sensitive to users' demand for privacy.

TABLE OF CONTENTS

"You have zero privacy. Get over it."
Scott McNealy, CEO, Sun Microsystems, 1999

INTRODUCTION

We are well into the digital information age. Internet, one of the most outstanding products of this age is affecting all of us in innumerable ways. The facilities offered by Internet ranges from a simple communication medium to a way of life. The World Wide Web (WWW) has attracted both business and non-business institutions that want to establish a foothold in the online world for reasons ranging from prestige, information dissemination to money-making. This mad rush to have an online presence has sometimes bordered on mass hysteria.

However, in this mad rush, one aspect of human life that everybody values has been ignored to a point of oblivion – Privacy. People are concerned about privacy, particularly on the faceless Internet. However, traditionally, business institutions with online presence have been reluctant in catering to the demands for privacy. As mentioned in [1], "making any promises about protecting customers' data would only expose them to liability". However, this is changing. As users are becoming more demanding and options are growing, businesses are being forced to reevaluate their stand on user privacy. Surveys have shown that fear of losing privacy is keeping customers off the Net, or at least preventing them from doing online business. In one survey [2], it was found that only 13% of the respondents reported that they were "not very" or "not at all" concerned about privacy on the Internet.

This reports looks at the issue of privacy from different angles. First it tries to identify what is personal information. Then it tries to analyze the ways in which personal information (PI) is mined on the Internet and what the end users can do to stop the leakage of unwanted information. Special mention is given to medical privacy since it is one of the most sensitive of the private information that can fall in wrong hands. The report then presents the result of a privacy survey conducted on Singapore based websites. It was found that on an average, Singapore based sites are not too sensitive to the privacy concerns of its users, and are resorting to use of privacy threatening cookies and other technologies. In the end, initiatives by bodies and organizations related to online privacy are studied.

"That – control of the information once its leaves the individual hands- is what the issue is all about"

Esther Dyson, Chairman, Electronic Frontier Foundation [1]

WHAT IS PRIVACY?

A value worth keeping

Defined broadly, privacy is the protection of personal information (PI) such as one's address, social security number, email address, credit card history, tax records and medical records of our visits to the doctor or the results of medical tests. Privacy is a personal preference. What the author considers private, the reader may consider as public knowledge. However, there is some information that each one of us would choose to keep private. Even more challenging is that fact that there is some information we would like to release to selected few people, with the confidence that it will not be passed around. According to Esther Dyson, that is what is the core of the problem.

As expected, a study [2] revealed that online users have various comfort levels across varying personal information. People were found to be more comfortable with providing information about their preference (like favorite TV show or snack) than with revealing sensitive information like phone and credit card numbers. As an extension the study also showed that the public in general was more concerned if the information was obtained from a child.

Who uses PI?

How did our personal information become so valuable? Who uses our PI? There are questions whose answers we require to make any meaningful legislation on privacy. There are various levels of institutions that value our PI. Companies want information on its customers so that they can make profitable decisions. The ability to identify the taste and dislikes of its customers can help a company to streamline its products, as well as make its advertising more targeted.

Credit card companies would like to know our spending style to decide whether to extend limit. Book selling companies would like to follow users' reading habits so that they can recommend books that are more of their liking, improving the probability that the user would buy the advertised book. Insurance companies would want to know of our medical history so that they can know if they are getting into a potential risky deal with our insurance. Governments want to track citizens' personal information so that they can enforce law and order and protect national security.

However, it should be added that, as pointed out by Paul Sholtz [3], there is a misconception that advertisements fuel the Internet. If this were so, as rightly pointed out, companies like DoubleClick would already have shown profit. It is the PI that runs the show. This is evident in the way companies like DoubleClick has been shifting their business model from just delivering ads to collecting PIs and selling them to other business institutions.

"It is the one-way mirror effect that makes people nervous"
Esther Dyson, Release 1.0 [4]

PRIVACY THREATS

In this section, the report looks at the different methods that the PIs gatherers use to reap information from online users.

Cookies
Cookies are small files stored on the hard disk of the user. They can be used by websites to store tidbits of information. It has existed since 1995 when Netscape Navigator 1.1 was released. Initially it was merely intended to be a way to personalize a website during time of visit and not to be stored on user's computer [5]. The cookie default can, however be overwritten and the original inoffensive cookies are being used for difference purpose altogether.

Cookies can be used to keep track of user's motion through a website, the amount of time one spends on each section, the links that are followed and various other details. Most of the time the sites themselves use these cookies. But some companies that manage online ads can track user activity across all their client sites. For big advertising companies like DoubleClick, these sites may number thousands. Many users are not aware that they have cookies on their machines since websites commonly do not notify the use of cookies. Among those who know about the cookies many still don't know about its ability to be persistent.

However, awareness has been increasing. This can be judged by the fact that both Netscape and Microsoft Internet Explorer have made important changes with respect to user's ability to control cookies. The combination of increased public awareness of cookies usage (seen in the proliferation of methods to surf anonymously) with possible government intervention to safeguard user privacy in Internet has forced a lot of changes in the way cookies are used. The new cookie standard [6] (RFC 2965) is aimed at quenching some of the concerns regarding the use of cookies. However for these to be put into practice would require some time and until then user would have to make use of other ways to guard privacy.

Web Browser Extensions
Microsoft Internet Explorer (IE), one of the most widely used web browsers, has the ability to use downloadable web browser extensions that extend the working of IE. Some of the extra functionalities these extensions provide include the ability to fill out web forms, perform price comparison and to liven up the interface with thematic images. A summary of browser extension products is available in [7]. However, most of these extensions are offered free of charge in exchange for 'clickstream' and profile information about the user and access to the user's display for advertising.

A study [8] showed that most of the extensions that were studied, 'phoned home' more data than is necessary for the functionality as offered and disclosed to the end user at download time. They found out that out of the 16 extensions studied, more than 50% monitored the URLs visited by the user. Not only does this reveal information on the kind of websites that the user visits, but also provide more information on what exactly is it that the user is searching for, on the web. When a user searches for information on various search engines on the web, an inspection into the string obtained can reveal the search query. Many exten-

sions listen to these query string and phone home the data hoping to gather information that may have profit or shopping value. Even though most of the extensions use these gathered information for customizing the ads that are shown to the user, there is enough potential for misuse, to warrant concern.

Medical record privacy

Among the various thefts of privacy possible, theft of personal medical record is one of the most serious and most feared. Clinical medicine is highly information intensive, and is one of the few areas of our society where computer access to information has been highly limited, to areas like billing and scheduling, laboratory result reporting and diagnostic instrumentation system. However, the move to the widely accepted electronic patient records (EPR) is accelerating and so is the fear of exposing patient's highly private and sensitive information to unauthorized eyes.

Studies [9] have shown that most important threats to patients records comes from:

- Accidental disclosure
  Unintentional mistakes made by medical personnel that can cause accidental disclosures.
- Insider curiosity
  Medical personnel abuse their record access privilege out of curiosity or the willful intention of abuse.
- Insider subornation
  Medical personnel can willfully release sensitive information for motives ranging from revenge, spite and profit.
- Unauthorized access
  Network intruders can break into patient record system and steal sensitive information. A study in 1997 however found no examples of outside intruder break-ins [9]. However results of these studies must be taken with a pinch of salt, since medical institutions may not be forthcoming on the details regarding any successful attacks that may have occurred. Added on that would be the fact that the study was conducted in 1997 when Internet was still in a nascent state. Given the number of successful attacks on so many machines connected to Internet including military sites, it is highly unlikely that there would be no attacks on medical systems.

Monitoring by Employers

In most countries employees have little or no privacy protection from monitoring by employers. There are several ways in which employers can monitor employees' computer.

- Employers can use software that can record the data appearing on a user's computer screen and even stored in their hard disks.
- Keystroke monitoring can give an indication to the employer as to how much work is being done by an employee involved in intensive word processing work.
- Employer can keep a log of emails sent from workplace.

If an electronic mail (e-mail) system is used at a company, the employer owns it and is allowed to review its contents. Messages sent within the company as well as those that are sent from employee's terminal to another company or from another company to the employee can be subject to monitoring by the employer. The same holds true for voice mail systems. Several workplace privacy court cases have been decided in the employer's favor (See for example, Bourke v. Nissan, Shoars v. Epson, and Smyth v. Pillsbury [10]). Even

when user deletes message from his/her terminal, they are still kept in the system. Although it appears like they are erased, they are often permanently "backed up" on magnetic tape, along with other important data from the computer system.

Big Brother & Privacy

New communication medium opened by the emergence of Internet has provided substantial advantage to the law enforcement agencies of the government. From the information released by the FBI, the 'Carnivore' system of the US Government is "capable of capturing any TCP/IP application (i.e. SMTP, FTP, TELNET)" over a range of networks [11]. Since e-mail messages are often stored with a service provider for a period of time before they are read by the intended recipient (and even sometimes after they are read), e-mail is less transient than telephone calls and thus more vulnerable to interception. Law enforcement can intercept a person's e-mail and other Internet activity in real time, by monitoring the phone line that serves as most people's connection to the Net. Computers have made it possible for law enforcement agencies to analyze vast amounts of information about personal communications patterns far more easily. Pen registers, which recorded the numbers dialed on a particular phone line, have been superseded by multiline dialed number recorders, and these, in turn, have been computerized, allowing agencies to automatically search for revealing patterns of calls.

As a result of the recent terrorist attacks on America, more expanded wiretap authorities have been proposed. It is also being proposed that all cryptographic products built in America should have backdoors installed which will give the government the ability to decode any coded message.

Financial Privacy

Internet has become one of the latest mediums for conducting business. There are different levels of business transactions that take place on the Internet. Business to Business (B to B) and Business to Consumer (B to C) are among the most important of these levels. Among the two, B to C transactions is the ones, which raises privacy concerns. When a user conducts a transaction over the web, many things can go wrong. If the site is not a secure one, user's information, like name, password and credit card number can be obtained by snooping software. An unscrupulous merchant can record down the credit card number in the merchant's server before passing it to the bank and misuse it at a later stage.

Many banks, mortgage brokers and insurance companies fail to fully inform online customers of their privacy rights. Some pass their online customers' financial information to telemarketers, travel agents, credit-card vendors, and junk-mail-generating retailers without the customers' knowledge or permission. According to a survey conducted by Washington-based Center for Democracy & Technology, of the 100 financial companies surveyed:

- 80 provided online customers little or no advice on how to limit the sharing of their financial information.
- 34 shared their online customers' financial information with unaffiliated companies without telling the customers they were doing so.

"Thousands of Singaporeans sign on to the Net every month, despite worries over personal privacy in this efficiently policed state."

Ravi Velloor, TIME Special Report, October 11, 1999

PRIVACY SURVEY OF SINGAPOREAN SITES

A number of surveys have been done to quantitatively analyze the privacy practices of the various web sites on the Internet. However, the focus of most of these surveys has been sites based in USA, since most of the popular sites are based in USA. In this section we present the results of the survey conducted on the privacy policies of sites related to Singapore.

Methodology

In conducting the survey two specific attributes were looked for. It was checked if the website was placing a cookie on the user's computer when the user is visiting the main page of the site. The logic for doing this is that, as the page being visited is the main page of the site, the user would have no idea of the privacy policy of the site and the privacy practice being followed by the site. Furthermore the main page of a site is usually a general page giving details of the services offered by the site rather than a member specific site, which might warrant the use of a cookie. A distinction was made on the kind of cookie being used. Some of the cookies placed were from the sites themselves while other were of third party site, mostly ad serving companies.

The second attribute that was looked for was whether the site had a privacy policy at all and if it has, whether it is present in the main page of the site at a place that is easily visible to the user. To check if a site had a privacy policy at all, the following procedure was adopted. First it was checked if a direct link to privacy practice was available from the front page. It is usually linked as either 'Privacy' or 'Terms of Usage'. If there were no mentions of these on the front page, the string 'Privacy' was searched for using the site's search engine (if there was one). If a search revealed any section on privacy practice of the site, the site was regarded as having a privacy policy, but the difficulty in finding the policy was noted. The survey was conducted in the first week of October 2001 and the details may have changed after that.

Results

The detailed survey result is presented in Appendix A. The results of the survey are summarized and analyzed in the rest of this section. 40 Singaporean websites were examined for this survey. The sites ranged from government agency sites to commercial banks, entertainment and media sites. The sites were chosen at random but care was taken to ensure that these were popular sites so that the relevance of the survey could be preserved.

Out of the 40 sites, 19 placed cookies in the user's machine on entering the front page of the site, while 16 sites had no privacy policy at all. A surprising find was that the website belonging to government agencies and departments fared badly. It was found that www.sg, www.iras.gov.sg and www.moe.gov.sg did not have a privacy policy. Furthermore, moe.gov.sg placed a cookie when a search for word 'privacy' was performed. Website of both universities in Singapore fared badly too. While the website of Nanyang Technological University did not have any privacy policy, the site of National University of Singapore not only did not have a privacy policy but also used cookies in its front page.

Almost all the commercial websites used cookies, but most of them had links to their privacy policy from the main page. Out of the four banking sites surveyed, only DBS Bank website did not have a privacy policy section and except for Citibank; none seemed to be using cookies on the front page. This is quiet comforting considering the fact that most of the Internet population of Singapore does use Internet banking facilities of the respective banks.

BuzzCity (www.buzzcity.com.sg) had an interesting privacy policy. Stated in the 'Privacy Policy' were the following:

"*BuzzCity may keep you informed by fax, post, email or free messages about other products or services and may disclose your personal data to other companies for this purpose. Unless you specifically state otherwise, you consent to the use and disclosure of your personal data for this purpose."*

"BuzzCity may at its sole discretion collect data and prepare reports regarding your use of the Service and shall keep such information confidential unless otherwise required."

Even though it is stated that the site will 'keep such information confidential' it is followed by the vague condition 'unless otherwise required'. Another disturbing policy is the 'default opt in' policy rather than the more appropriate and user-friendly policy of 'default opt out'.

Another interesting observation from the survey data was that two of the websites that had privacy policy, specifically mentioned that they were logging the IP address of the users' machines. What makes this process murkier is the fact that it is not mentioned as to how the collected information will be used. In the extreme case, the log of IP address can be used to track individual users.

Suggestions

Overall, it can be said that even though most commercial Singapore based sites do address the privacy concerns of the users in one way or the other, there are a number of improvements that can be made. The privacy policy can be made to reflect 'default opt out' rather than a 'default opt-in' policy. When detailed logs are being made (like IP logs), the users can be informed as to how these will be used. Rather than stating that the privacy policies can change and the user has to keep visiting the privacy page for changes, the registered users should be informed by email, any change in the privacy policy. It has been widely suggested that the first page of a website should not place cookies on a machine. The rational is that since this is the first page, a user visiting the site would not have had the opportunity to examine the privacy policy of the site and make a well informed decision as to whether he/she agrees to abide by the policy. Sites that are not having any privacy policy at all should do so, even if they do not use cookies and other intentional means of logging usage. This is because, by default, most of the web servers do IP logging and privacy conscious users may like to know how the information is being used.

"The technology is developing at the speed of light, but the privacy laws to protect us are back in the Stone Age"

Barry Steinhardt, Associate Director, American Civil Liberties Union

PROTECTING ONLINE PRIVACY

There are various methods in which online users can protect their privacy from prying eyes. This section of the report details some of them.

Cookie Busters

As mentioned previously, cookies are an important way of tracking online users. There are various cookie management software and services that give the users more control over the cookies. One example is the 'Internet Junkbuster Proxy [12]. It runs on Win95/98/NT/2000 and Unix. It can selectively block cookies for the user allowing the user to specify permission to cookies on a per site basis. Muffin [13] and interMute [14] are other cookie management software that has gained wide usage among privacy conscious people.

There are numerous 'cookie cutter' or 'cookie eater' applications, which can be programmed to run at regular intervals to clean the cookie files. Other options that can be used are the 'infomediary' such SeigeSoft's SiegeSurfer [15]. These products act as a proxy between user and the visiting site, intercepting all cookies and disguising the real user. "The best solution: full cookie management built into the browsers themselves" [16] is also on its way. Microsoft Internet Explorer 6 has and Netscape 6 have a lot of extra cookie management functionalities built into it.

Spam Fighters

Anyone who has been online for more than a couple of months and have used an email address would have encountered 'spam' or unsolicited bulk email. When a privacy conscious user receives a spam, one of the first thing he might try to do is to unsubscribe by replying with "REMOVE" in the subject line, or other un-subscription information provided in the email. This simply confirms the fact that the user's email address is being read by a real person!

There are variety of filters and anti-spam services available that can help tackle the problem of Spam. The following are some of them:

- Spam Hater (http://www.cix.co.uk/~net-services/spam/span_hater.htm) for Windows users
- TAG (http://alcor.concordia.ca/topics/email/auto/procmail.spam) for Unix users
- SpamCop (http://www.spamcop.net)
- Brightmail (http://www.brightmail.com/individual/)

'Clean' email address

Spammers get hold of user's email address by hunting through newsgroups, html pages, mailing lists, chat rooms and other public places on the web. Hence it is prudent to use an alternate throwaway email address for all these places. One should use the 'real' email address only to communicate with known trusted individuals and close, personal friends. When choosing free email service providers as primary email service, one should read the privacy policy carefully, as a lot of free offers come with poor privacy and track records.

Shop at secure web sites
Since most of the online shopping that is done involve the passing of user's credit card and other personal information, it is necessary to make sure that the site that one is using is a secure site. A secure site uses encryption technology to transfer information from the user's computer to the server. Information like credit card number, username, password, and name are scrambled using the encryption technology. There are several ways in which one can know if a site uses encryption technology to secure the transactions. If the URL of the site is of the form 'https://', the site is using encryption. The 's' stands for 'secure'. Another way to check for secure nature of a website is to look out for the closed padlock displayed on the bottom of the browser window. If the padlock sign is open it can be assumed that the site is not secure.

Of course, transmitting user's data via secure channels is of little value to the user if the merchant stores the data unscrambled. The user should attempt to determine if the merchant stores the data in encrypted form, so if a hacker is able to intrude, he would not be able to obtain user's credit data and other personal information. The user should read the merchant's privacy and security policies to learn how it safeguards your personal data on its computers.

Realization of being monitored
Users have to realize that it is more likely than not that; they are being monitored at work. Currently there are very few laws regulating employee monitoring. Privacy conscious user should avoid sending very personal email at work, except if it is work related. Users also need to be aware that an increasing number of employers are monitoring and recording employee web usage, as well as email. This could compromise home banking passwords and other sensitive information. Users should keep private data and private net usage private, at home.

Encryption
Encryption is a method of scrambling an e-mail message or file so that it is gibberish to anyone who does not know how to unscramble it. The privacy advantage of encryption is that anything encrypted is virtually inaccessible to anyone other than the designated recipient. Thus, private information may be encrypted, and then transmitted, stored or distributed without fear that outsiders will scrutinize it. The online service system operator, or anyone else who has obtained the message legally or illegally cannot read an encrypted e-mail message. Therefore, any message containing private or sensitive information should be encrypted prior to communicating it online. Various strong encryption programs, such as PGP (Pretty Good Privacy) are available online [17].

Because encryption prevents unauthorized access, law enforcement agencies have expressed concerns over the use of this technology, and Congress has considered legislation to create a "back door" to allow law enforcement officials to decipher encrypted messages. Users should be aware that the legal status of this technology is still unsettled. Moreover, federal law limits exporting certain types of encryption code or descriptive information to other countries.

"Hold tightly to the hand of Nurse, for fear of finding something worse."
Hillaire Belloc, poet

LAW, AGENCIES & PRIVACY

There has been a lot of work going on with the intention of protecting user privacy on the Internet, both from governments and also consortium of leading companies.

Government Initiative
In June 1997, the US Federal Trade Commission's (FTC) Bureau of Protection conducted a workshop on consumer Information Privacy to determine if federal legislations are required to ensure privacy of users on the Internet or whether Internet business can be relied on to satisfy privacy concerns. Among other topics, FTC hearings raised awareness of the importance of privacy concerns and seemed to culminate to a period where online registration and cookies were perhaps more tolerated because of less awareness. As set forth in *A Framework for Global Electronic Commerce*, the Clinton administration showed support for private sector efforts to implement meaningful, consumer-friendly, self-regulatory regimes to protect privacy.

In May 2000, FTC issued the 'Final rule on privacy of consumer financial information' [18]. "The Rule imposes on financial institutions three main requirements established by the Act. First, a financial institution must provide to its customers a notice about its privacy policies and practices. That notice must be clear, conspicuous and accurate and must describe the conditions under which a financial institution may disclose nonpublic personal information to nonaffiliated third parties and affiliates. Second, a financial institution must provide its customers with annual notices of its privacy policies and practices. Like the initial notice, the annual notice must be clear, conspicuous and accurate. Third, a financial institution must provide consumers with a reasonable opportunity to "opt out" of disclosures of their nonpublic personal information to nonaffiliated third parties and a reasonable means by which to opt out. Consumers may exercise their right to opt out at any time."

The Department of Commerce of USA is encouraging industry to demonstrate its solutions to privacy problems and promoting its effort to public. The Federal Trade Commission is however growing a bit impatient. The US Government has been telling the public and a variety of foreign governments that the Net can govern itself. Now these cheerful assurances seem to be fading. But there are several silver linings. Two of the bodies that try to do this are discussed below.

TRUSTe
With the slogan of 'Building a framework for global trust' [19], TRUSTe, a non-profit organization tries to ensure that user's privacy is protected through open disclosure and empowers users to make informed choices. TRUSTe was established in 1996 by the Electronic Frontier Foundation and Commcercent. It is a standard for disclosure, a labeling system, and an auditing/recourse mechanism. But aside from some best-practices regarding children, it leaves licensee free to do what they want with their customer's data – as long as they disclose their practices and follow their promises. This point has to be understood properly. If a site has TRUSTe seal, it does not mean that customer data is secure. What it means is that, there exists enough audits and checks to ensure that the policy laid down on the website is strictly followed.

Whether overall or tailored, if a site boasts of TRUSTe seal, its privacy statement discloses, at a minimum:

- What type of information the sites gathers
- How the site uses the gathered information
- Who the site shares the information with
- Whether the users can correct and update their personally identifiable information
- Whether users will be deleted or deactivated from the site's database upon request
- Whether user can opt out of giving specific information to third parties

When there is a problem, it can arise either through user's complaint or TRUSTe's auditing. First TRUSTe would send a formal notice and gives the target an opportunity to respond. If the response is inadequate, TRUSTe can pursue it according to contract – revoking the license and the mark, auditing the miscreant (at the licensee's cost) and publicizing the results. If the break appears willful and fraudulent, TRUSTe can call in the local jurisdiction under which the license was signed and sue. TRUSTe can also call in Federal Trace Commission of USA or other government agencies in serious cases.

BBBOnline

BBBOnline is a wholly owned subsidiary of Council of Better Business Bureaus. According to the website [20], BBBOnline's mission is to 'promote trust and confidence on the Internet through the BBBOnline Reliability and BBBOnline Privacy programs. BBBOnline's website seal programs allow companies with websites to display the seals once they have been evaluated and confirmed to meet the program requirements. The BBBOnline Reliability Seal confirms a company is a member of their local Better Business Bureau have been reviewed to meet truth in advertisement guidelines and follows good customer service practices. The BBBOnline Privacy Seal confirms that a company stands behind its online privacy policy and has met the program requirements regarding the handling of personal information that is provided through its website. The BBBOnline Kid's Privacy Seal is found on websites and online services that comply with an extensive collection of additional requirements that address the unique online privacy issues associated with young children.

Platform for Privacy Preferences Project (P3P)

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium [21], is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

CONCLUSION

This report looked at the issue of user privacy in the Internet age. After defining the meaning of privacy, the report shed light on the various threats to user privacy in this age of information highway. This included cookies, browser extensions and government policing among others. Special mention was given to medical privacy since it is one of the most sensitive of the private information that can fall in wrong hands. Then the result of the privacy survey conducted of Singaporean sites was presented. It was seen that out of the 40 sites, 19 placed cookies in the user's machine on entering the front page of the site, while 16 sites had no privacy policy at all. It was felt that Singaporean sites were becoming sensitive to user's privacy, but much needs to be done. Next, various methods of protecting online privacy was discussed including use of software and also various bodies and agencies.

In conclusion it can be said that slowly but steadily, web sites are becoming more sensitive to users' demands for privacy protection. Business establishments are recognizing the fact that privacy concerns of consumers are preventing them from using the Internet to its full extent. Various laws and legislations are being put in place to safeguard user privacy. However, it has been seen that since these extra steps involve time and money, they will be implemented only if users press for them. The future of user privacy is in the users' hands. If we, as users stick to our demand for a fair, regulated privacy practice, the commercial institutions will be forced to concede to them.

REFERENCES

[1] 'Privacy Protection: Time to Think and Act Locally and Globally', Esther Dyson, First Monday.

[2] 'Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences', Mark S. Ackerman, Lorrie Faith Cranor, Joseph Reagle, ACM Conference on Electronic Commerce, 1999.

[3] 'Economics of Personal Information Exchange', Paul Sholtz, First Monday.

[4] 'Release 1.0', Esther Dyson.

[5] 'Persistent Client State HTTP Cookies, Preliminary Specifications', Netscape Communications Corporation, 1995.

[6] 'HTTP State Management Mechanism', RFC 2865, D. Kristol, L. Montulli, IETF.

[7] '30 Ways to browse better', Mendelson E, PC Magazine 19, (Oct. 2000).

[8] 'The Privacy Practices of web browser extensions', David M. Martin Jr., Richard M. Smith, Michael Brittain, Ivan Fetch, Hailin Wu, Communications of the ACM, February 2001, Vol. 44, No.2.

[9] 'For Record: Protecting Electronic Health Information', National Research Council, 1997.

[10] See http://www.law.seattleu.edu/choum/privacy.html

[11] EPIC Carnivore FOIA Documents, http://www.epic.org/privacy/carnivore/

[12] Internet Junkbuster, http://www.junkbuster.com

[13] Muffin, http://www.muffin.doit.org

[14] interMute, http://www.intermute.com

[15] SiegeSurfer, http://www.siegesoft.com

[16] 'EFF's Top 12 ways to Protect Your Online Privacy', Santon McCandlish, Electronic Frontier Foundation.

[17] Pretty Good Privacy, http://www.pgpi.org

[18] 'Final rule on privacy of consumer financial information', Federal Trace Commission (USA), http://www.ftc.gov/opa/2000/05/glbpress1.htm

[19] TRUSTe, http://www.truste.org

[20] BBBOnline – http://www.bbbonline.org

[21] World Wide Web Consortium, http://www.w3.org

APPENDIX A – SURVEY OF SINGAPOREAN SITES

Site Name	URL	Privacy Policy	Cookie	Comments
DBS Bank	www.dbs.com.sg	No	No	
OCBC Bank	www.ocbc.com.sg	Yes	No	
Keppel Bank	www.keppelbak.com.sg	Yes	No	
Citibank SG	www.citibank.com.sg	Yes	Yes	
Catcha SG	www.catcha.com.sg	Yes	Yes	Cookie from ad company
Yahoo SG	sg.yahoo.com	Yes	Yes	
Yellow Pages	www.ypcommerce.com	Yes	Yes	
Microsoft SG	www.msn.com.sg	Yes	Yes	
SG Computer Society	www.scs.org.sg	No	No	
Strait Times	straitstimes.asia1.com.sg	Yes	Yes	
Asia One	Asia1.com.sg	Yes	Yes	
Interauct	Interauct.com.sg	Yes	No	
Juz Swap	www.juzswap.com	Yes	Yes	Ad company and hit counter cookie
Business Times	Business-times.asia1.com.sg	Yes	Yes	
Buzzcity	Buzzcity.com.sg	Yes	Yes	Poor Privacy Policy
Movies Online	Movies-online.com.sg	No	Yes	Pacfusion Ad cookie
Asia Food City	www.asiafoodcity.com	No	Yes	Users need to register for using services, but there is no Privacy Policy
HardwareZone	www.hardwarezone.com	Yes	Yes	Cookie from 2 ad companies. Privacy Policy says IP logging occurs.
IT Street	Itstreet.com.sg	Yes	No	
Job Street	www.jobstreet.com.sg	Yes	No	
GetAsia	www.getasia.com.sg	Yes	Yes	Ad Cookie, IP logging.
Singapore Infomap	www.sg	No	No	
Gov. of SG	www.gov.sg	Yes	Yes	Website search puts a cookie
MOE	www.moe.gov.sg	No	Yes	Website search puts a cookie
Media Corp	www.mediacorp.com.sg	Yes	No	
Network for Electronic Transfers	www.nets.com.sg	Yes	No	Privacy policy found through search. No direct link from main page
IRAS	www.iras.com.sg	No	No	
Nanyang Technological University	www.ntu.edu.sg	No	No	
National University of Singapore	www.nus.edu.sg	No	Yes	
Singapore Management University	www.smu.edu.sg	No	No	
National University Hospital	www.nuh.com.sg	No	No	
Singapore General Hospital	www.sgh.com.sg	No	No	

Singapore Air-lines	www.singaporeair.com.sg	Yes	No	
Changi Airport	Changi.airport.com.sg	No	No	
Shaw	www.shaw.com.sg	No	No	
Golden Village	www.goldenvillage.com.sg	No	No	
SISTIC	www.sistic.com.sg	No	No	A lot of information needed for registra-tion but there is no privacy policy
Singnet	www.signet.com.sg	Yes	Yes	Ad & other cookie.
Starhub	Starhub.com.sg	Yes	No	
Pacific Internet	Pacific.net.sg	Yes	Yes	Ad cookie