JITTA
JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION

PRIVACY DISCLOSURES OF WEB SITES IN TAIWAN

HENG-LI YANG, National Cheng-Chi University
Department of Management Information Systems, College of Commerce, 64 Section 2, Chihnan Road, Mucha Dist., 116, Taipei, Taiwan. Tel: +886-2-29387651. Fax: +886-2-29393754. Email: yanh@mis.nccu.edu.tw

HSIEN-KUEI CHIU, Jin-Wen Institute of Technology
Department of Management Information Systems, 99 An-Chung Road, Hsin-Tien, 231, Taipei, Taiwan. Tel: +886-2-82122330. Fax: +886-2-86662223. Email: hkchiu@ms9.hinet.net

ABSTRACT

This research involves two phases. In the first phase, 339 ".com.tw" and 15 major ISP sites located in Taiwan were examined, in order to draw a picture of the status of Web-site privacy disclosures. The results showed that most of them failed to meet the requirements of the Fair Information Practices. More than 80% of them did not show their privacy policies, and more than 30% failed to provide any statements regarding information privacy practices. Less than 10% of the Web sites explained how privacy concerns might be satisfied and what channels might be utilized for complaint. Over 80% did not display security or privacy seals. Among the Web sites collecting personal ID numbers, credit card numbers and birth dates, only 20% declared their privacy policies. The findings indicate that in comparison to the U.S., the importance of privacy disclosures has not been widely recognized in Taiwan. Sequentially, in the second phase, this study conducted in-depth interviews with the Web-site managers to reveal the possible disclosure determinants. Besides, the possible cultural impacts on Taiwan Web-site privacy practices have been discussed. Finally, some recommendations are given.

Rajiv Kishore acted as senior editor for this article.

Yang, H., and H. Chiu, "Privacy Disclosures of Web Sites in Taiwan", *The Journal of Information Technology Theory and Application (JITTA),* 4:3, 2002, 15-42.

INTRODUCTION

E-Commerce technology has developed rapidly. The development of information technologies (IT) has allowed businesses to analyze the information they collect and thus to profile their customers. Many commercial Web sites collect personal information while customers shop or browse them, even though the information might not be necessary to fulfill a transaction. Exposed to the potential threats of unauthorized personal information usages, Web users or consumers are increasingly concerned with what personal information Web sites collect, how the sites use and control the information, and what security protections the sites provide.

To examine the privacy practices of Web sites in Taiwan, a survey was conducted to investigate the contents of online shopping Web sites, free Web resources providers, and major ISP Web sites. The privacy issues involved in the Web site contents include: (1) What kinds of information are being collected (the information that users are required to fill out)? (2) Are users informed that the system would collect information, which users did not explicitly provide, but could be obtained during the system operation process? (3) Are users informed about where and how the collected information will be used? (4) Are users asked to consent to secondary usages of information, i.e. usages unrelated to the original purpose for which information was collected? (5) Do the Web sites obtain consent from information owners regarding how the collected information will be shared with other organizations? (6) Are users informed about where the collected

CONTRIBUTION

This paper makes a contribution to IS research in the following ways.

1. To our knowledge, it is the first study to comprehensively examine the status of privacy protection disclosures of Taiwan Web sites. Also, the study is the first to explore the reasons why the Web sites disclose or do not disclose their privacy protection policies or practices.
2. The paper provides a comparison of the extent to which various privacy features are present in the Web sites located in Taiwan and the United States. A model is developed to categorize the features to help in the comparison.
3. This paper is also the first report to compare non-ISP shopping sites with ISP sites that keep a large number of real customers. Our study shows that, even though the proportion of ISP Web sites that disclose their privacy policies or practices is greater than that of ".com.tw" Web sites, the ISP sites do not fully satisfy customers who are concerned about personal privacy and transactional security.
4. The study provides the evidence that most Web sites located in Taiwan failed to meet the requirements of the Fair Information Practices. This suggests that the Taiwanese authority should refine the Computer-Processed Personal Data Law of 1995 and help construct a creditable authentication environment of e-commerce, in compliance with the requirements for information privacy protection in the global/internet market.
5. Regarding the benefit to e-commerce, this study provides CEOs and IS managers a complete checklist of privacy protection disclosures and some possible factors leading to a low privacy disclosure rate. Besides, it also stimulates the third parties that provide authentication seals to ponder the reason why the seal disclosure rate is low.
6. This research is expected to appeal to those readers, who are concerned about the issues of information privacy, and would like to capture a picture of the status of Web-site privacy disclosures in Taiwan, or those who hope to know the decision factors on privacy disclosures behind the Web sites. The knowledge provided in this paper is useful not only for local readers but also for global readers who are interested in cross-national/cultural comparisons.

information will be stored, and how it will be protected?

In addition, this research intended to (1) discover whether ISP Web sites, which possess enormous amounts of sensitive information, would pay more attention to privacy disclosures than other commercial sites; (2) compare our findings with those from the U.S.; and (3) explore the possible reasons involved in the decision framework behind the status of privacy disclosures.

LITERATURE REVIEW

Information and Right to Privacy

The concept of privacy can be traced back to the article "The Right to Privacy" of Warren and Brandeis (1890). Justice Brandeis of the U.S. Supreme Court stated that the right to privacy is "the right to be left alone - the most comprehensive of rights, and the right most valued by civilized men[1]." Westin (1967) defined the right to privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Clarke (1999) pointed out "information privacy refers to the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use."

Liu (1988) suggested that protection of the right to privacy should focus on the following: (1) restrictions on information collection, (2) accuracy of information, (3) the right to inquire and modify one's personal information, (4) the right to receive notice of information collection, (5) the right to know the existence of information and so on. He further discussed the threats posed by computers to privacy by categorizing them into two aspects, the IT aspect and the social psychology aspect. The rapid development of IT made collection, storage and retrieval of information fast and easy, so that the maintenance of privacy became more difficult. As for the social psychology aspect, one may be disadvantaged and disturbed by another's illicit access and exploitation of personal information, and use of out-of-date or false information.

Wang *et al.* (1998) indicated that privacy, in the context of consumers' or Web users' E-commerce activities, often relates to personal information. Invasion of privacy is often interpreted as the unauthorized collection, disclosure or illicit use of direct results of online transactions. As far as personal information privacy is concerned, there are two types of personal information. One is static private information that is unlikely to change significantly over time, such as historical financial data, religious beliefs and so on. The other is dynamic personal information that changes significantly over time, such as the moving tracks and their contents.

According to Milberg *et al.* (1995), regulatory models regarding privacy issues can be classified into *No Information Privacy Regulation* (e.g., Thailand), *Self-Help* model (e.g., France), *Voluntary-Control* model (e.g., Japan, U.S.), *Data-Commissioner* model (e.g., Australia, Canada and New Zealand), *Registration* model (e.g., Demark, U.K.), and *Licensing* model. Milberg *et al.* indicated that all corporate uses of personal data are more likely to be regulated in a country where the government has a higher level of involvement in corporate privacy management, and to its extreme, the government has the authority to license those uses of personal data.

Banisar (2000) pointed out, to protect privacy, a country might use one or more of the following models: *Comprehensive laws, Sectoral Laws*, *Self-Regulation*, and *Technologies of Privacy*. For instance, The European Union (EU) has adopted the "*Comprehensive laws"* model to ensure compliance with its data protection regime. The US has taken the "*Sectoral Laws"* model to protect privacy industry by industry (Givens 1997; Banisar 2000; Kramer 2002). Also, the US has applied the "*Self-Regulation"* model to companies and industry bodies in establishing

[1] The U.S. Supreme Court, Olmstead v. U.S., 277 U.S. 438 (1928).

the standard for data protection (Banisar 2000; Kramer 2002).

In the past, the US Federal Trade Commission (FTC) believed that self-regulation alone would adequately protect consumers' online privacy. However, in 2000, the FTC recommended that the US Congress enact legislation for adequate protection of consumer privacy online, since the industry's efforts to curb data privacy abuses had been disappointed (Banisar 2000; Kramer 2002). Meanwhile, as a major trading partner of the EU, the US felt that it was imperative to bridge the differences between the privacy approaches adopted by the EU and the US. Therefore, the US Department of Commerce in consultation with the European Commission developed a "safe harbor" framework for the US organizations to comply with the EU Directive. According to the US Department of Commerce, the decision by the US organizations to enter the safe harbor is entirely voluntary. To qualify for the safe harbor, an organization can join a self-regulatory privacy program that adheres to the safe harbor's requirements, or develop its own self-regulatory privacy policy that conforms to the safe harbor (U.S. Department of Commerce 2002).

Along with privacy concerns of people and world trade partners, some countries in the Asia Pacific region have proposed or enacted their new laws regarding privacy issues (Banisar 2000; White & Case LLP 2002). Banisar (2000) pointed out "the movement towards comprehensive privacy and data protection laws for a country might be due to the following reason(s): to remedy past injustices, to promote electronic commerce, and/or to ensure that laws are consistent with Pan-European laws." The main reason for many Asia Pacific countries to develop new laws is to promote electronic commerce. They have their own non-English languages and cultures, and recognize that consumers might be uneasy with their personal information being sent out worldwide. Some examples of law enactment regarding data protection are as follows:

In Thailand, six bills (E-commerce law, EDI Law, Privacy Law Data Protection Law, Computer Crime Law, Electronic Digital Signature Law, Electronic Fund Transfer Law and Universal Access Law) were submitted to the Cabinet in 2000. In Japan, with regard to general privacy, and protection of private information, a proposed amendment to the existing law was submitted to the Diet in 2002. Hong Kong enacted its Personal Data (Privacy) Ordinance in 1995 and most of its provisions took effect in 1996. This Ordinance imposed additional restrictions on certain processing. For instance, data matching required the prior approval of the Privacy Commissioner. As for Singapore, a code focused on data protection has been proposed recently in 2002.

Taiwan has departed from a plight of "*No Information Privacy Regulation"* toward an environment close to *"Comprehensive law"*, since the government enacted the Computer-Processed Personal Data Protection Law (CPPDPL) in 1995. The CPPDPL governs data processing by public as well as non-public institutions. It establishes separate principles for eight categories of non-public institutions: credit information organizations, hospitals, schools, telecommunication businesses, financial businesses, securities businesses, insurance businesses, mass media, and "other enterprises, organizations, or individuals designated by the Ministry of Justice and the central government authorities in charge of concerned end enterprises." However, it fails to cover other categories of the users like individuals or legal entities whose business activities involve the collection, processing, and use of information available on the Internet (Greenleaf 1998; STLC 2002). Unlike Hong Kong, there is no privacy commissioner and no single privacy oversight body to enforce the CPPDPL. The Ministry of Justice enforces the CPPDPL for government agencies, and other relevant government agency enforces the compliance of the private sector. Besides the CPPDPL, there are other laws and regulations in terms of privacy, such as Article 12 of the *Constitution*, Articles 18, 184 and 195 of the *Civil Law,* Article 318-1 of the *Criminal Law,* Articles 6 and 56-1 of the *Telecommunications Law.* In 2001, Taiwan enacted the Digital Signature Law to enhance e-commerce security in business transactions.

Privacy Policy Concerning Personal Information Protection

Killingsworth (1999) suggested that given a framework of information security and integrity, the "consensus approach" to personal information privacy is a market-oriented model, where consumers or Web users are involved in decision-making about disclosure and use of their personal information. The US FTC separated elements of the *Fair Information Practices* into *Notice*, *Choice*, *Access*, *Security*, and *Enforcement*.

"Notice" refers to whether a consumer or Web user is given clear and accessible notice, prior to personal information being collected by the Web site. Is there notice of the type of personal information being collected, how it is collected, and how it will be utilized (such as objective, scope or purpose of use)? Is there notice of whether the Web site will inform its user when cookies are used, whether personal information may be deleted upon request, and whether the user may request that sending of emails be stopped? Are users of the Web site reminded of their self-responsibility towards privacy protection? Is there an explanation as to the consequences of refusing to provide information?

"Choice" refers to the condition that a consumer or Web user is given options, when an application of information might go beyond the scope of user's original provision. A "choice" might include an "opt-in" or "opt-out". For instance, is a Web user given the right to choose whether to be contacted? Is there a statement mentioning whether the Web site might disclose the collected information to a third party? Is the Web user given the "choice" to agree or disagree on such disclosures of information? Is there an explanation as to what types of third parties (e.g. advertisers, business partners or other companies) will be given the information? Is there a general statement provided, e.g., "provision of information to third parties is in aggregate form, and not as individual records"? If "individual records" will be provided, can the user choose which parts of the information may be disclosed or withheld?

"Access" refers to the condition that a consumer or Web user is allowed reasonable access to the information stored about him/her, and is given the right to modify or even delete any inaccurate information.

"Security" refers to whether there is any statement regarding the protection of personal information during the process of transmission from a client's PC to a Web server. Is there any statement as to what measures and steps would be taken by the Web site to protect personal information after transmission?

"Enforcement" refers to the effective enforcement of the principles mentioned above. In addition, a privacy policy should also provide "*contact information*" so that a Web user can contact the Web site's operator, in case that he/she would like to submit any queries or complaints about this Web site's handling of the privacy issues.

The US privacy laws emphasize the *Fair Information Practices*. This means that without notifying relevant parties and obtaining their prior consent, holders of information should not use information provided by the public for a specific purpose towards a different purpose.

The US FTC introduced in 1998 the final version of the *Children On-line Privacy Protection Act* (COPPA), which requested more "Notice" and "Consent" requirements for those commercial Web sites or ISPs that may be linked or may collect information on minors under the age of 13. The US has also enforced the *Gramm-Leach-Bliley Act* to require financial institutions to clearly disclose their privacy policies on their annual financial reports (FTC 1999, 2000; Microsoft 1999).

Empirical Studies on Privacy Policy in the US

Culnan (1999a, 1999b)[2] has conducted two separate surveys on privacy protection by Web sites. One selected a random pool of 361 ".com" commercial Web sites from the top

[2] These studies are also referred to as the "Georgetown Internet Privacy Policy Survey" (GIPPS) and the "Online Privacy Alliance Report on the Top 100" (OPA), respectively.

7,500, and the other surveyed the top 100 ".com" commercial sites. Both surveys contained the following three main questions: (1) What kinds of personal information do Web sites collect from consumers? (2) How many Web sites provide privacy disclosures? (3) Do such disclosures adequately reflect the *Fair Information Practices*?

The results of the studies showed that with respect to personal information collection, 92.8% of the 361 Web sites collected personal identifying information (such as ID numbers and email addresses, etc.), and 56.8% collected demographic information (such as age / date of birth, education and preferences/interests, etc.). 98% of the top 100 Web sites collected personal identifying information, while 75% collected demographic information.

Regarding privacy disclosures, 34.1% of the 361 Web sites provided no related statement whatsoever, 22.4% merely provided an *information practice statement* (e.g., "click here, if you do not wish to receive emails from us"), while 43.5% (157/361) disclosed a *privacy policy*. 6% of the top 100 Web sites provided no related statement, 12% merely provided an information practice statement, while 81% (81/100) disclosed a privacy policy.

Out of the 361 Web sites, 236 collected personal information and disclosed how they managed privacy issues. Among these Web sites, the percentages in containing at least one kind of disclosure of "Notice", "Choice", "Access", "Security", and "Contact Information" were 89.9%, 61.9%, 40.3%, 45.8%, and 48.7%, respectively. Out of the top 100 Web sites, 94 collected personal information as well as disclosed how they managed privacy issues. The percentages of these Web sites containing at least one kind of disclosures of "Notice", "Choice", "Access", "Security", and "Contact Information" are 93.5%, 83.1%, 50.3%, 51.6% and 59.1%, respectively.

In a follow-up study (FTC 2000), the US FTC randomly sampled 335 sites and also investigated 91 of the most popular Web sites in 2000. Besides the questions studied in the earlier research, a few more topics were added, such as the disclosure of cookies posted by third parties (e.g. advertisers) to a Web site, and the display of a *privacy seal*.

The FTC (2000) study found that in the *random samples*, 12% of the sites provided no disclosure and 62% posted a privacy policy. In the *most popular group*, all of the sites contained at least one disclosure and 97% posted a privacy policy. These posting rates were higher than those in the previous year, indicating that the U.S. commercial Web sites were placing greater importance on disclosures of privacy policy. However, the study showed that 57% of the sites in the *random samples* and 78% of the sites in the *most popular group* allowed the placement of cookies[3] by third parties. Furthermore, the majority (78% and 49%, respectively) of these Web sites, which allowed the placement of cookies by third parties, did not disclose that fact to consumers. As for enforcement, there were severe limits on the extent and effectiveness of calls for privacy protection from the self-regulatory seal programs. Only approximately 8% of the sites in the *random sample* and approximately 45% of the sites in the *most popular group* displayed privacy seals on their Web pages. Clearly, there was a lack of popular participation in the online privacy seal system introduced by the self-regulatory programs. Therefore, the FTC pointed out that there was still room for improvements in these programs, and also recommended the US Congress to enact privacy protection laws. Not only should consumer-oriented commercial Web sites be brought under the regulation of COPPA, but also there should be clearer legislation to demand all such Web sites to comply with the four widely accepted requirements set out in the *Fair Information Practices*.

A few issues have not been dealt with in the above studies. Some are as follows. (1) Do Web sites log users' browsing activities? (2) Beyond law requirements or protection of legitimate third parties, are there

[3] In order to investigate whether third parties (such as advertisers) utilized cookies, the FTC (2000) study set the status of browsers to "notify user". Whenever a third party utilized cookies, a warning page would pop up to notify the user.

circumstances under which a Web user has the choice to agree on information sharing to third parties? (3) If information sharing to third parties is not in aggregate form but includes "individual records," does the user have a "choice" as to revealing certain personal information?

RESEARCH FRAMEWORK

This study suggests a privacy disclosure framework as shown in Figure 1. The conceptual and operational definitions of the variables are in Table 1.

RESEARCH METHODS AND DESIGNS

Instrument Overview and Research Design

There are two phases in this research. In the first phase, a survey questionnaire was designed to investigate the status of Web-site privacy disclosures. Research assistants consisted of one doctorate candidate and one master student in Management Information Systems, and both of them had taken computer and technology law courses. The research assistants browsed online shopping Web sites to observe the status of Web-site privacy disclosures, and recorded their observations in accordance with the items on the research questionnaire.

The questionnaire was adapted from Culnan's studies and FTC reports. Some modifications had been properly made to provide a more complete understanding of the status of Web-site privacy disclosures in Taiwan. Some items had been added in the questionnaire to examine the disclosures of Web-site privacy practices, such as: explaining the ways to delete personal information and providing an option to cancel membership; reminding Web users of their responsibilities for privacy protection; explaining under what exceptional circumstances personal information will be disclosed; explaining what types of or which third-party Web sites will share personal information; presenting an option of what fields in the records of personal information may be disclosed; explaining what warranties the Web sites can provide in case of no Opt-ins or Opt-outs for privacy disclosures; explaining what specific ways to deal with inaccuracies in personal information collected; and displaying a licensed "security seal" and/or a licensed "privacy protection seal." This research has separated the security seal from the privacy seal since security transmission and transaction were given more attentions in Taiwan.

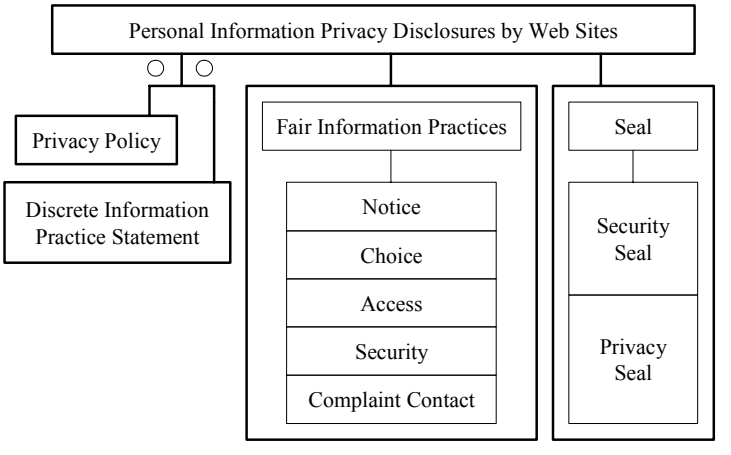

Figure 1. A Framework for Privacy Disclosures[4]

[4] The notation "◯" in Figure 1 means "or", i.e. disclosures of a Web site may be either "privacy policy" or "discrete information practice statement".

Table 1. Definitions of Variables Surveyed in This Study

Variable	Conceptual Definition	Operational Definition
Privacy Policy Disclosure	There is a unified (comprehensive) description of a Web site's practices regarding personal information protection policy, which should be easily seen by anyone.	Some comprehensive statements by a Web site regarding personal information protection measures are located on either the home page, or the home page containing an icon or hyperlink leading to such statements. If not, when some personal information is being collected or is required to be filled in, the statements should appear. Otherwise, as the last resort, the statements may appear on other related pages (e.g. customer services) in the Web site.
Discrete Information Practice Statement	There is a discrete statement by a Web site regarding personal information protection measures, which should be easily seen by anyone concerned in this issue.	There is at least one statement regarding personal information protection measures. This statement is clearly displayed on the Web page where data are being collected or are required to be filled in, or the user can be led to such a statement by clicking on an icon or hyperlink. Otherwise, as the last resort, the statement may appear on other related pages (e.g. customer services) in the Web site.
Notice	The Web site informs the user prior to collecting personal information.	"Notice" should include the following information: Types of information being collected, means of collection, purposes of collection, utilization of cookies, means of deleting personal information, means of stopping sending of E-mail advertisements, and self-responsibility.
Choice	Users have the right regarding whether to allow the collected information being used for purposes exceeding the scope of original purposes.	"Choice" should include the following: Click to choose whether to be contacted by a Web site operator; click to choose whether personal information will be available to third parties; click to choose the kinds of third parties allowed to access to personal information; whether aggregate information is made available, and if not, click to choose disclosures of items in individual records.
Access	Users have reasonable access to information stored about them.	"Access" should include the following: personal information may be reviewed and modified; dealing with inaccuracies in information.
Security	Web site operator's protection of information during data transmission and storage.	"Security" should include the following: explanation of transmission security, internal security measures for control and management of information.
Contact Information	Explanation regarding channels for concerns or complaints related to privacy.	"Contact information" should include the following: statement of contact channels for privacy concerns; explanation of complaint channels for infringement of privacy.
Security Seal	Licensed seal for secured transactions.	A Web page displays the secured transaction seal licensed by a certain security seal program, and users can click on the seal to verify whether that particular shopping Web site is the one whose global security has been recognized.
Privacy Seal	Licensed seal for Personal information privacy protection	A Web page displays the "privacy protection seal" licensed by a certain privacy protection seal program.

The questionnaire consists of five parts. The first part focuses on a collection of basic personal data by Web sites, and investigates what kinds of personal identifying information and demographic information Web sites collect, as well as whether they maintain a user's browsing activity logs. The second part examines where there are privacy policy disclosure statements. The third part checks out where there are information practice disclosure statements. The fourth part is concerned with the contents of privacy disclosures, which is categorized into four elements in accordance with the *Fair Information Practices*: general "Notice," "Choice," "Access," "Security," And "Contact Information."

Most of questions in the questionnaire are close-ended. The research assistants were required to record objectively whether a Web site contained statements or functions related to privacy. Most questions require simple answers of "yes" or "no". Depending on the answers, the research assistants might skip to other questions or answer secondary questions.

In the second phase we conducted in-depth interviews with the managers of five chosen Web sites. Each interview covered three aspects: (1) the manager's self-reporting on the questionnaire of our first phase, and his/her explanations for the reasons of disclosing or not, (2) how the site used customer data, (3) how the sites actually protected its customer privacy. Except for the questionnaire of the first phase, other questions of the second phase are open-ended.

Sampling Processes and Data Collections in the First Phase

Subjects and Sample Frame

The subjects of this study were ".com.tw" shopping Web sites, sites that provided free Web space or e-mailing services, and major ISP Web sites.

The samples of ".com.tw" were gathered from various sources: the Web sites categorized as "online shopping" or "free e-mailing service" in the most popular portal site — Kimo, plus shopping Web sites found through keyword search by three most popular search engines—Kimo, Yahoo! and Yam in July 2000. The names listed increased to 1335 sites at this stage. Then we added 156 online shopping sites that introduced themselves in an e-Oscar campaign conducted by http://www.e-oscar.com.tw. Finally, we deleted redundant sites (341), not ".tw" sites (380), ".net" and "net.tw" sites (148), pornographic Web sites (16), no longer existing or inaccessible sites (43), and the sites that merely provided descriptions of the company or its products without collecting personal information (224). The remaining number of the sites was 339, out of which 19 provided free resources.

With respect to online privacy protection by major ISP Web sites, this study selected 15 ISP Web sites which together account for 98% of the combined allowable subscriber base, an estimate of the total number of subscribers (CFCT 1999). Except for New Silk Road Technology, which accounted for less than 1% of the allowable subscriber base, all others account for at least 1%. Furthermore, most of these 15 ISPs had at least 1% of the total Internet connection accounts in Taiwan.

Survey Process

The visits to all 339 Web sites took place in two stages from July to September 2000. This was due to the fact that there was a large number of Web sites and limited research personnel. In the first stage, from July to August 2000, research assistants browsed Through all of these sites one by one to answer our privacy questionnaire. Then, in the second stage, from September 1 to 7, 2000 the assistants double-checked them again to ascertain whether the Web sites had modified their privacy disclosures. The purpose of the second stage is to assure that the comparisons among the Web sites were in the same period of time.

The Reasons for the Comparison between Shopping Sites and ISPs

ISPs in the past primarily provided connection services, but now they also provide co-location and Web hosting as well as ASP services, or may even establish Internet Data Centers ("IDC"). In fact, ISPs have already entered the diversified domains of e-commerce, and therefore, the online shopping function has become one of their services. As

Table 2. Top 15 Internet Service Providers

Chung Hua Telecom Digital, branch (Hinet)	www.hinet.net
Digital United Inc.	www.seed.net.tw
GC Technologies (GC Net)	www.gen.net.tw
ERA Internet Enterprise	www.eranet.net
TisNet (Tatung Internet) (Tisnet)	www.tisnet.net.tw
Apache Inc. (Apol)	www.apol.com.tw
United Tech (MyNet)	www.my.net.tw
Union International Telecom Value-added Network Service (FICNet)	www.ficnet.net
Infoserve Inc. (IS.NET)	www.is.net.tw
Sysnet Inc. (Sysnet)	www.sysnet.net.tw
Pagic.net Inc. (PAGIC.Net)	www.pagic.net
Instant Access Telecommunications Network Corp.	www.timenet.net
Asurveyo Information Network (seeder.net)	www.seeder.net.tw
Giga Media Ltd. (Giga Super Network)	www.giga.net.tw
New Silk Road Technology Inc.	www.silkera.net

a result, ISPs possess their own databases of sensitive information about their customers or these customers' clients. Compared to shopping sites, most ISPs have larger customer databases that contain relatively true information, and are more regulated by the Telecommunications Law. Based on this perspective, ISPs should pay more attentions to privacy issues.

Some of the ".com.tw" Web sites that originally provided free Web resources now also provide online shopping functions, due to their Web popularity in terms of mass membership. However, unlike ISPs, these Web sites are not bound by the strict Telecommunications Law. Therefore, this paper combines free Web resource sites with shopping Web sites, and then compares them to ISP Web sites.

Validity and Reliability of the Questionnaire

Considering the content validity of the questionnaire, we derived the questions from the literature (Culnan 1999a, 1999b, 2000; FTC 2000) as well as the opinions of some legal and information system experts[5]. Prior to formally commencing the research, the researcher and two research assistants read through the questions one by one, in order to ensure consistent understandings. In addition, the research assistants had been given advanced training[6], so that even if Web sites expressed their privacy statements in different ways, the assistants would have uniform standards of definition and evaluation. For the reliability of the research results, two pre-test surveys were conducted to verify the stability of the standards and to improve the uniformity of evaluations between the research assistants. In each pre-test survey, research assistants

[5] The legal and information system experts include two senior and remarkable professors in National Cheng-Chi University, Taiwan. One is an expert in the technology laws & the intellectual property rights, and also a director of the graduate school of technology management, as well as a founder of the graduate school of intellectual property rights. The other is an expert in management information systems, and has published many papers in distinguished journals.

[6] One of research assistants has been a PhD student in MIS with minor in Intellectual Property Rights of E-commerce. The other was a master student at that time and has earned his master degree in MIS. He had taken a 3-credit course of Computer Law before the survey was conducted. Before this survey has begun, both of them have been given three weeks to understand the studies of Culnan(1999a,199b) and FTC(2000).

Table 3. Personal Information Collected by Web sites

Information Collected	".com.tw" Web sites (339)		ISPs (15)	
	No. Web sites	% Web sites	No. Web sites	% Web sites
Personal ID Number	207	61.1%	15	100%*
Credit card number	167	49.3%	15	100%*
Credit card expiry date	167	49.3%	15	100%*
Name	337	99.4%	15	100%
Alias	53	15.6%	1	6.7%
Gender	209	61.7%	7	46.7%
E-mail address	287	84.7%	10	66.7%
Postal address	293	86.4%	15	100%
Permanent address	16	4.7%	0	0%
Contact phone number	294	86.7%	15	100%
Fax number	96	28.3%	12	80%*
Date of birth	219	64.6%	8	53.3%
Marital status	66	19.5%	1	6.7%
Education	118	34.8%	5	33.3%
Hobby/interest	55	16.2%	1	6.7%
Income	82	24.2%	2	13.3%
Occupation	140	41.3%	9	60%
Web user activity log	15	4.4%	4	26.7%*

Note 1: The content of a Web-user activity log includes the IP address, the path of browsing, and the time of sign-in and sign-out, etc. In the last row of "Web user activity log" of this table, the value merely indicates that there were 15 related statements mentioned in these Web sites. This study did not investigate a Web site's actual operations of logging. Some other sites might actually make such activity logs.

Note 2: The sign "*" indicates that given a significance level of $\alpha = 0.05$, the percentage difference between ".com.tw" commercial Web sites and ISP Web sites is significant.

separately investigated 20 Web sites that were randomly selected from the sample frame. At the end of each pre-test, the results obtained by the two research assistants were compared, so as to clarify the standard and reconcile differences. The inter-rater coefficient was improved from 94% in the first pre-test to 99% in the second.

RESEARCH FINDINGS IN THE FIRST PHASE

Detailed Findings

The findings of this study are grouped into ".com.tw" and ISP Web sites for comparison. Then we assess whether there is any significant difference between these two groups at a significance level of $\alpha = 0.05$.

Table 3 shows the details of personal information collection by Web sites. Table 4 shows the status of Web sites' disclosures of privacy policies and information practice statements.

Finding Summary

(1) Low disclosure rate of privacy policy: As shown in Table 4 and Figure 2, most of the ".com.tw" sites and ISP sites did not disclose their privacy policies on their Web pages. Even out of those 49 (14.5%) ".com.tw" sites that did have such policies, 18 sites only provided them on pages that were not obviously found.

(2) Low disclosure rate of privacy policy on the sites collecting sensitive information: As shown in Table 5, out of those 167 ".com.tw" sites which collected credit card information, a majority (80.2%) failed to disclose their privacy policies on their Web pages. Out of those 30 Web sites that collected all of personal identification number, credit card information, birth dates

Table 4. Disclosures of Privacy Policy and Information Practice Statements

Questions	% of all Web sites making disclosures	
	"com.tw"	ISP
Privacy Policy		
1. Is a unified privacy policy statement displayed on the Web site?	14.5%	26.7%
2. Can the privacy policy statement be viewed on the home page, or is there a linkage on the home page leading the user to a separate privacy policy statement page?	6.8%	20%*
3. Does at least one Web page collecting personal information link to a "privacy policy statement", or the page itself displays such a statement?	7.1%	20%
Information Practice Statement		
4. Does the Web site only display one or more discrete information practice statements (not a unified policy)?	48.9%	73.3%*
5. Does at least one Web page collecting personal information link to an "information practice statement", or the page itself displaying such a statement?	41.3%	73.3%*
Notice		
6. Notice of what personal information is being collected?	11.5%	26.7%
7. Notice of how personal data are being collected?	8.6%	20%
8. Notice of how personal information will be used? (e.g. objectives, scope or purposes)	19.2%	26.7%
9. Does the Web site inform its users of the use of cookies?	9.4%	26.7%*
10. Is there an explanation of whether personal information may be deleted at any time?	2.7%	6.7%
10a. If "no" to 10, are users informed of the option to cancel membership?	5.9%	6.7%
11. Notice of an option to request not receiving e-mails from the Web site?	11.2%	6.7%
12. Reminder of a Web user's self-responsibility for privacy protection?	26.5%	86.7%*
13. Is there an explanation of consequences of not providing information?	1.2%	20%*
Choice		
14. Is there a statement mentioning the possibility that the Web site or its affiliated organization may use the collected information to contact consumers or Web users, for marketing or other purposes?	22.7%	33.3%
15. In conjunction with 14, do Web users have the right to "choose" whether to be contacted?	14.7%	26.7%
16. Is there a statement mentioning the possibility that this Web site may reveal to third parties the collected information? (If "no", skip to 22; if "yes", continue to next question)	16.8%	33.3%
16a. In conjunction with 16, is the revelation made only under exceptional circumstances? (e.g. statutory requirement, request by judicial body, or to protect a legitimate third party)	11.8%	33.3%
17. Other than the exceptional circumstances described in 16a, does a Web user have a "choice" to agree or disagree to disclose to third parties the collected information?	5.3%	33.3%*
18. Other than the exceptional circumstances described in 16a, is there an explanation regarding which or what types of third parties the collected information will be disclosed to? (e.g. advertisers, business partners, or other companies)	2.1%	13.3%*
19. In conjunction with 18, does a Web user have a "choice" to disclose or not disclose information to certain or certain types of third parties? (e.g. advertisers, business partners, or other operators)	0.3%	0%

Table 4. Disclosures of Privacy Policy and Information Practice Statements (Cont'd)

20. Does it state that information provided to third parties is in aggregate form, and not as individual records? (If "yes", skip to 22; if "no", continue to next question)	3.2%	26.7%*
21. In conjunction with 20, if information is provided as "individual records", does a Web user have a "choice" as to which personal information may be disclosed?	0.0%	0%
22. If "no" to both 14 and 16, does the Web site provide any following warranty: (1) warrant not to disclose to third parties; (2) warrant to comply with relevant laws and regulations; (3) warrant not to infringe the right to privacy; (4) warrant not to use for any other purpose; (5) warrant to abide by social standards; (6) others. _____.	15.6%	13%
Access		
23. Does a Web site allow users to review or raise inquiries about personal information collected?	62.8%	93.3%*
24. Is there an explanation of how to deal with inaccuracies in personal information collected? (1) would be directly deleted by Web site; (2) users must make their own checks and rectifications; (3) appeal to laws; (4) others _____.	24.2%	33.3%
25. Is there an explanation as to how personal information may be modified?	53.7%	86.7%*
Security		
26. Is there an explanation as to protective measures for data transmission processes from a client PC to a Web server site?	36.6%	53.3%
27. Does the Web site state that it will protect personal information after its receipt?	8.3%	20%
28. In conjunction with 27, is there a substantive explanation of measures or steps?	0.6%	6.7%*
Contact Information		
29. Does the Web site explain how it may be contacted in the event of any queries concerning privacy?	3.5%	20%*
30. Is there any explanation how privacy complaints about this Web site or other organizations may be dealt with?	0.3%	13.3%*
Seal		
31. Does it display a licensed "security seal"?	17.7%	6.7%
32. Does it display a licensed "privacy protection seal"?	0.6%	0%

Note: (1) An "*" indicates that given a significance level of $\alpha = 0.05$, the percentage difference between ".com.tw" commercial Web sites and ISP Web sites is significant.
(2) More than one option may be selected in items 22 and 24, the percentages are those taking any one.

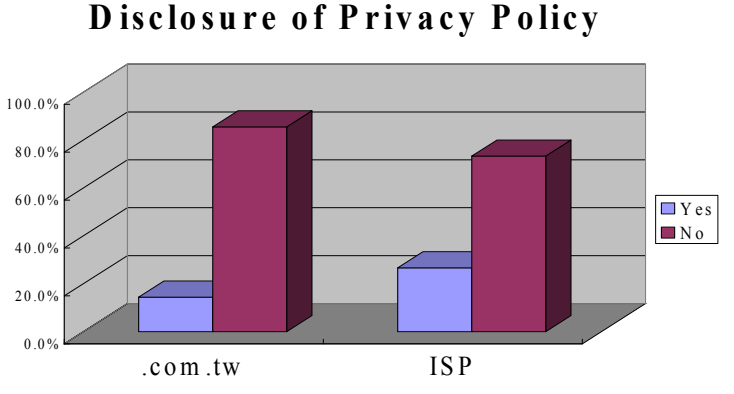

Figure 2. Disclosure of Privacy Policy by Web Sites

and personal preferences, only 30% disclosed their privacy policies to consumers.

(3) Low disclosure rates of fair information practices and seals: On average, as shown in Table 6, the disclosure rates of fair information practices and seals were low. Among them, the rate of "Access" was the highest, since Web sites allowed members to edit their register information. A few Web sites mentioned their security mechanisms of data transmission such as SSL.

(4) Lack of the explanation of the use of cookies: A great majority lacked any explanation regarding whether to use cookies or not. Such explanation would be important to consumers or Web users who were concerned with privacy issues and did not know how to turn off the cookies function.

(5) Low disclosure rates of the right to choose: 22.7% (i.e., 77) ".com.tw" sites mentioned that their sites or their affiliated organizations might use the information collected for contacting consumers or Web users, for marketing or other purposes. However, 29 of these sites did not provide the contact choices. Moreover, fewer sites provided other choices, as shown in Table 6.

(6) Privacy statements expressed in the interest of the Web sites: Some Web sites (11.8% of the ".com.tw" sites and 33.3% of the ISP sites) not only declared privacy protection statements, but also contained certain exceptional clauses. Such exceptional clauses included: "for the purpose of protecting the rights and interests of the company". This would allow a great deal of flexibility, which might give rise to certain problems, such as: if the Web went bankrupt, could the collected information be sold to other companies without the permission of the interested parties? Would a Web site sacrifice the rights and interests of its customers for its own operational benefit? Under these circumstances, consumers might appear to be at a disadvantage, which might be in conflict with the principles of reciprocity and good faith.

Table 5. Sites Collecting Sensitive Information and Their Privacy Policy Disclosures

Collecting information type	Number of sites that didn't disclose their privacy policies	%	Number of sites that disclosed their privacy policies	%	Total number
ID number	173	83.6%	34	16.4%	207
Credit card number	134	80.2%	33	19.8%	167
Age and birth	176	80.4%	43	19.6%	219
Hobby and interest	42	76.4%	13	23.6%	55
Collect all of the above	21	70.0%	9	30.0%	30

Table 6. The Disclosure Rates of Fair Information Practices and Seals

Fair Information Practices and Seal Disclosure (On Average)[7]	% of all Web sites making disclosures	
	".com.tw"	ISP
Notice	10.69%	25.21%
Choice	9.25%	21.29%
Access	46.90%	71.10%
Security	15.17%	26.67%
Contact Information	1.90%	16.65%
Seal	9.15%	3.35%

[7] For instance, the disclosure rate of "Notice" came out from the number of "Notice" items disclosed divided by the number of all samples.

15.6% ".com.tw" sites and 13% ISP sites merely gave ambiguous statements, such as, "promise not to disclose to third parties," "promise not to infringe the right to privacy," "promise not to use for any other purpose" or "absolutely confidential" and so on.

(7) The limited access to personal information: Although 62.8% of the ".com.tw" sites allowed users to access their personal information, such access was limited to membership information that users originally entered. In general, users were not allowed to access their activity logs. We also found that some Web sites even did not allow users to review their own past history of transactions.

No Web site would automatically correct any inaccuracies (e.g., out-of-date, input errors, or deliberate falsifications) in the information already collected. However, 24.2% of the ".com.tw" Web sites notified users of their policies towards inaccurate information. Some would directly delete or cancel the user's membership, while others would require users to renew their personal information periodically and voluntarily.

(8) Much less care for the security measures after information transmission than during process of information transmission: 91.7% ".com.tw" sites and 80% ISP sites did not mention protecting the security of information after transmission. Even if they talked about any security issue, they provided no detailed explanations.

(9) Loose contact and unsound complaint channel: Only 3.5% ".com.tw" sites and 20% ISP sites clearly stated that users might e-mail to the Web sites for discussing their privacy concerns. Very few (0.3% ".com.tw" sites and 13.3% ISP sites) explained how users could register complaints.

(10) Much less seal disclosure and focus only on transmission security rather than various personal information protection issues:

This survey found that only 17.7% (60) ".com.tw" sites displayed a security seal. Most of the disclosed security seals were HiTrust security seals. Others were one TaiCA seal, two SecureOnline seals, and one Thawte seal. Only the HiTrust seal provided a hyperlink that enabled a user to verify whether the shopping site was a really secure Web site. However, on 12 such sites displaying HiTrust seals, when we actually clicked on their security seals, there were no responses. It might suggest that the sites never actually applied for seals, or had not gotten their renewals.

Only two Web sites had "privacy protection seals" approved by SOSA. Clearly, Taiwanese shopping Web sites still lacked a popular and objective "third party" to accredit their online privacy protections.

FINDING DISCUSSIONS

Comparisons between .com.tw and ISP

ISP Web sites have some similarities in comparison with shopping Web sites, such as collecting personal information, providing shopping services, providing the solution of on-line payment, demanding customer information for marketing planning, doing business within the internet, and demanding the information security and personal information protection. However, ISPs Web sites also have some differences as compared to shopping Web sites. These differences imply that ISPs have more valuable information and are expected to have better performance of security and privacy protection than non-ISP shopping Web sites. Troublesome spamming might happen if ISPs release personal information (e.g. e-mail addresses) to advertisers or other parties. Besides, in addition to Web users, a company also needs to pay close attention to its ISP's security and privacy policy, if it stores any valuable information on its Web servers and those servers are housed at an ISP (Radcliff 1998). These differences are as follows:

1. Most of the ISPs are run by larger companies. Besides, many non-ISP shopping Web sites have no support from physical companies.
2. ISPs have been more regulated by Taiwan government than the pure shopping sites.

3. Security serves as one of the main services of ISPs rather than just an enhancement to business and transaction fulfillment.
4. ISPs need to track user activity to detect user traffic and to trace malicious traffic if necessary, but shopping sites do not.
5. A lot of personal and company information is transmitted through and stored in ISPs, and many companies store their valuable information in their servers that are located at ISPs.
6. ISP value-added services for companies fall into three categories: complexity management, increased security and improved performance (Morri 1998).
7. ISPs allow on-line customers to apply for Internet services, pay their telephone bills, and purchase limited dial-up service packages.
8. ISPs are capable of playing other roles such as portal sites and data centers.
9. ISPs provide a variety of services, e.g. in forms of basic service, e-commerce (shopping stores), advertising, messaging service, travel and fun, access, search engine, yellow pages, money and finance, and public service, etc.

As shown in Tables 3 & 4 of the survey, some findings are as we expected. They are summarized as follows:

1. The ISP Web sites were more likely than the ".com.tw" Web sites to collect personal identifying information such as ID numbers and credit card numbers. This might be because ISP Web sites required their membership applicants to provide accurate personal information for identification.
2. The ISP Web sites were more likely to provide a hyperlink of privacy-policy statement on the home page, and also to show privacy-protection statements on the Web pages where a Web user was requested to enter personal information. This might be because ISPs kept more customer information and they would be more concerned about privacy disclosures. In addition, they had more experienced personnel. Therefore, they were aware of providing easy access to the privacy disclosures for Web users.
3. With respect to general notices, the ISP sites were more likely than the shopping Web sites to notify users of their self-responsibilities for privacy protection. It seems that in Taiwan, an ISP was more serious than a start-up small shopping Web site. It also implies that from the innovation diffusion perspective, a shopping Web site launching into its business might have loose control over a Web user's usage at the beginning.
4. With respect to choice, if not considering some exceptional circumstances (e.g. statutory requirements, demands by judicial bodies or for protection of legitimate third parties), the ISP sites were more likely than the ".com.tw" sites to offer users the choice of whether to agree to reveal the collected information to third parties. Besides, the ISP sites were more likely than the ".com.tw" Web sites to state that disclosures of information to third parties were in aggregate or non-identifying form. This might be due to the fact that a larger ISP usually attracted many advertisers and worked with several strategic partners, and thus it would need its law department to review its public announcements related to third parties and Web users. In general, an ISP with law department would be more conscious of the necessity for obtaining customers' consent before distributing their personal information to third parties.

However, as shown in Table 4, a unified privacy policy was not popularly disclosed in either ISP or non-ISP shopping sites. Although the percentage in disclosing a unified privacy policy in the ISP Web sites was relatively higher, the difference was not statistically significant.

ISPs were less inclined to notify Web users of an option to refuse receiving e-mails from the Web site. During our interviews, a top manager of a popular ISP explained: "Instead of being disclosed on the Web site, this option was embedded in the content of e-mails that consumers had received. We

assumed that the Web-using consumers were willing to receive e-mails from us since they had filled in their e-mail addresses." As a matter of fact, the Web site first sent unsolicited commercial e-mails to consumers without obtaining their explicit consents in advance.

Besides, ISPs were less inclined to disclose privacy seals on their Web sites. The above ISP also explained: "Current seal programs are not creditable enough. We already have good reputation and the brand image of our company is much better than those of the seal programs." The situation reflects the fact that local privacy-seal programs have not been popular in Taiwan.

Overall speaking, the disclosures of Web-site privacy protection were not popular in Taiwan, regardless of ISP or non-ISP shopping Web sites. This situation was due to the fact that the entire e-commerce environment was not mature in Taiwan. For instance, the privacy law did not enforce Web sites to disclose their privacy practices. The operators of Web sites in Taiwan did not feel the seal programs were credible in general, and did not strongly perceive the tangible benefits from the seal programs.

Regarding the differences in privacy practices between two types of Web sites, the above discussions suggest that they might derive from the following major factors: the demand for data integrity, the brand image effect, and the regulations and laws for enforcement. ISPs demand more integrity of personal data in order to detect user traffic in case malicious traffic occurs. Some ISPs either have being run for a longer time than shopping Web sites, or have support and inherit the brand image from their physical companies. In addition, ISPs in Taiwan usually have larger scales of business. Thus, they might make light of a small local privacy-seal program. Finally, the higher disclosure rates on the ISP Web sites might imply the effect of law enforcement on ISPs since ISPs had been more regulated by Taiwan government than the pure shopping sites.

Comparisons of this Study of Taiwan with those of the US

In the U.S., the percentage in providing privacy-policy disclosures increased from 43.5% (group of 361 surveyed sites) and 81% (group of top 100 sites) in Culnan's studies (1999a, 1999b) to 62% (group of 335 random samples) and 97% (group of the 91 most popular sites), respectively. As a comparison, in Taiwan only 14.5% of ".com.tw" and 26.7% of ISP sites provided privacy policy disclosures. This may indicate that in Taiwan the self-regulatory programs are still in its infancy.

- Out of the 339 surveyed ".com.tw" sites, the percentages in containing at least one kind of disclosures of "Notice", "Choice", "Access", "Security" and "Contact Information" were 41.9%, 38.9%, 60.2%, 37.8% and 3.5%, respectively. All proportional figures except "Access" were lower than Culnan's studies (Culnan 1999a, 1999b).
- In the U.S., privacy-related seal programs include TRUSTe, BBBonline Privacy, CPA WebTrust and so on. These programs advocate the importance of online privacy, and demand that any Web sites must first obtain explicit consents before utilizing a consumer's personal information. They also apply mandatory measures of assisting consumers or Web users in resolving complaints of privacy infringements. According to the study by the U.S. FTC, 8% of its 335 random surveyed samples and 45% of the 91 most popular sites displayed the privacy-related seal (FTC 2000). However, our study found that only about 18% ".com.tw" sites displayed privacy or security seal. Also, as previously mentioned, the majority of them were security seals, and only 0.6% ".com.tw" sites had privacy seals. Therefore, so far, Taiwan has paid more attentions to transaction security protection than privacy issues (e.g., notices, choices, consents and complaints).

ONE FURTHER STEP --- IN-DEPTH INTERVIEWS IN THE SECOND PHASE

To find out the possible reasons for a Web site to disclose its privacy practices or not, we have conducted the second phase of the research by interviewing five sites in depth. The selections of ".com.tw" sites were based on their disclosure rates in the first phase of our survey. Two sites were chosen from the cluster of higher disclosure rate, one from the mediocre cluster and the other from the lower cluster. The fifth site was the top ISP in Taiwan.

Factors Influencing the Web site Privacy Disclosure

Based on the interviews, fourteen factors influencing the Web site privacy disclosure were found, and were further grouped to the external and internal environmental factors, as shown in Figure 3.

In Figure 3, the "decision process" refers to the decision-making process consisting of defining privacy issues and collecting related information, considering the fourteen factors, designing the alternatives of disclosures, and evaluating and finally choosing the alternatives. However, there are five gaps as follows:

- Gap 1 is the discrepancy between disclosure decision outcome and actual disclosures on Web sites. This gap might arise because of implementation resistances or different perceptions between decision-makers and Web system designers on the privacy disclosures.
- Gap 2 is the discrepancy between the disclosures and actual behaviors of privacy protection. Gap 2 would occur when a Web site would not be serious about its own disclosures.
- Gap 3 is the discrepancy between consumer expectations before browsing and consumer perceptions after browsing the Web site. Consumers might have some unrealistic expectations because of culture, social concerns, company images, or personal experiences, etc.
- Gap 4 is the discrepancy between a Web site's privacy disclosures and consumer perceptions of its privacy protection. This gap might arise because of different interpretations of disclosure words.
- Gap 5 is the discrepancy between consumer perceptions of a Web site's privacy protection and its actual behaviors of privacy protection. When the Web site does not actually follow its privacy disclosures, this gap would occur and the consumers might feel cheated.

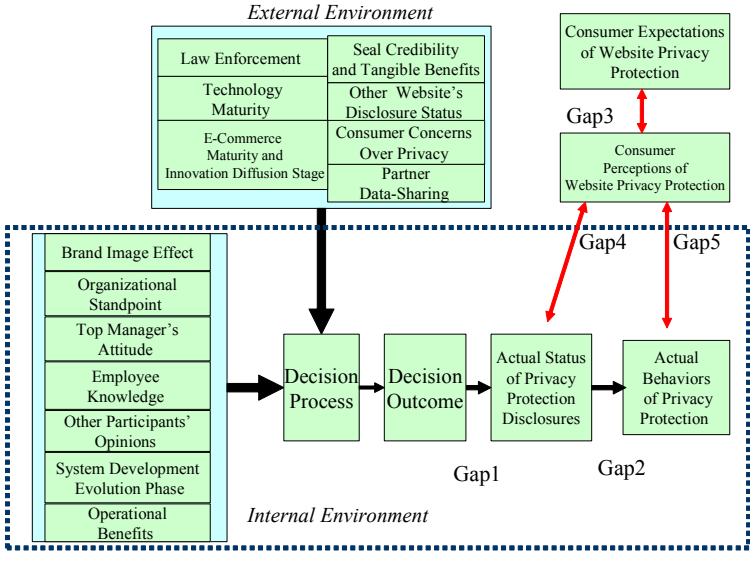

Figure 3. The Decision Factors on Disclosures and Possible Gap

Propositions and Discussions

In the following, we discuss the propositions implied by the fourteen external and internal environmental factors, and the gaps as shown in Figure 3.

(1) Law Enforcement

All of the interviewed Web sites agreed that the related laws were the most important determinants in making the disclosure of privacy practices. Despite there are the Computer-Processed Personal Data Law (CPPDL) and other laws regarding personal privacy in Taiwan, none of them has any strict demands on Web site privacy disclosures. In addition, the scope of CPPDL can only be applied to its listed industries. According to the Telecommunications Law in Taiwan, an ISP is stipulated as Category 2 of telecommunications business and thus it is naturally bound by the CPPDL; however, the regulation of other Internet businesses remains controversial from a legal standpoint of view. This also partially explains why the surveyed ISPs had higher disclosure rates than ".com.tw" sites. Besides, the lack of a set of detailed legal requirements and universal terminologies concerning the disclosure of privacy protection resulted in a variety of terms or degree of disclosures. Therefore, the lack of mandatory legal requirements tempted most Web sites to act with non-disclosure. This leads to:

> *Proposition 1: The higher the degree of law enforcement is, the higher the rate of privacy practice disclosure would be.*

(2) Technology Maturity

It would be necessary to inform the consumers of the possible risk of Web browsing and what privacy protection a site could provide in the absence of a dependable security mechanism on Internet. Therefore, we state:

> *Proposition 2: The less mature the applied technology of e-commerce (especially transaction security) is, the more important the disclosure of privacy protection practices would be.*

(3) E-Commerce Maturity and Innovation Diffusion Stages

Some sites might think that they had better not talk about sensitive topics like privacy in the current immature e-commerce market. However, we think that it would be necessary to establish consumers' confidence in this initial phase. Therefore, we postulate the following:

> *Proposition 3.1: The less mature the e-commerce market is, the less willing a Web site would disclose the privacy protection practices to customers. (Or the earlier stage of innovation Diffusion a Web site lies in, the less control on customer usage.)*

> *Proposition 3.2: The less mature the e-commerce market is, the more important it is to disclose the privacy protection practices to customers.*

(4) Seal Credibility and Tangible Benefits

Web sites would consider the direct tangible benefits of seal disclosures. The most common seal was the security seal verified by HiTrust, providing secured transmission of transaction data, whereas other seals did not offer the Web sites enough incentives to join in. Some Web sites might not know the seals or might think that some seals lack credibility. Therefore, here we state:

> *Proposition 4: The more credible and tangible benefits a seal can offer, the more inclined a Web site is to join in the seal program and post the seal on the Web site.*

(5) Other Web site's Disclosure Status

Some Web sites would tend to observe or even copy Web contents from other sites, especially in the same industry. They copied not only the business model of the most popular Web sites, but also their privacy practice disclosures. This leads to:

> *Proposition 5: The more popular a privacy practice disclosure is in the industry, the more likely a Web site is to disclose that kind of privacy practice.*

(6) Consumer Concerns Over Privacy

Though the disclosure rates were low, it did not mean the Web sites did not care about the consumers. Some sites just paid more attentions on marketing strategies or Web page designs. Others had already rationalized their non-disclosures in the following different ways: presupposing that the consumers might

be less inclined to read detailed descriptions, or might lack knowledge or involvement in claiming for personal rights of privacy, and also that too many disclosures inadvertently distract the consumers.

If the disclosures were regarded as little help to a customer accessing the Web site, they would more likely be neglected. They were such as mentioning that the site had collected what kind of consumer data or their browsing paths. On the contrary, a Web site would tend to disclose those that would be conducive to shopping. Those disclosures were such as how to enter personal information, or assuring security in data transmission. This may explain why the disclosure rates of "Access" and data transmission of "Security" (see Question 23, 24, 25 and 26 of Table 2) (functional designs) were higher than most of the "Notice" (plain descriptive texts) disclosure rates in our first phase of survey. Therefore, the disclosure decision would be influenced by general consumer concerns and involvement in privacy issues. Therefore, we postulate:

Proposition 6: The more attention a Web site pays to the consumer concerns over privacy, the higher disclosure rate of privacy practices it would have.

(7) Partner Data-Sharing

One of the interviewed managers said that the customers were encouraged to become the joint members of the Web site and its partners. Since this might involve data sharing, it would become necessary to disclose what partners and how these partners would use the collected customer personal information. Another interviewed Web site thought that the disclosure was necessary to clarify the responsibility of any advertisement sponsors who might collect and use the customer personal information. Thus, we state:

Proposition 7: The more possible it is to share data with strategic partners, the more necessary it is to disclose what types of data the strategic partners might receive and use.

(8) Brand Image Effect

A CEO of an interviewed ISP site did reiterate that the brand images of an ISP site and its satisfactory services would certainly outweigh the fastidious privacy policy descriptions. However, its legal department manager thought that the privacy disclosures could help enhance the Web site's image because it would highlight the firm's commitment to privacy protection in the modern society. Therefore, on one hand, a Web site with credible reputation might feel unnecessary to give detailed privacy protection disclosures. On the other hand, a popular Web site would also provide sufficient disclosures in order to maintain their long-established reputation. Therefore, we postulate:

Proposition 8: The better brand image a Web site has, the more confidence the customers have in the Web site.

(9) Organizational Standpoint

The reasons for disclosure, as found in the interviewed sites, were related to the organizational standpoint toward the privacy-related matters (such as legal issues, consumer concerns, competitors' privacy practices, technology availability, or seal programs). Therefore, we postulate:

Proposition 9: The stronger organizational standpoint toward privacy protection an organization has, the more its Web site would disclose privacy policy or information practice statements.

(10) Top Manager's Attitude

Some top managers put emphasis on the quality of Web-page design but, however, neglected the significance of information security and privacy protection. Therefore, the top manager's attitude toward privacy issues would be positively correlated to the status of the Web disclosure. In other words, we hereby state:

Proposition 10: The top manager's attitude toward privacy issues is positively correlated to the disclosure rate of privacy protection practices.

(11) Employee Knowledge of Privacy Protection

The non-disclosure would often be associated with ignorance of privacy protection. However, even if a person with such knowledge might choose non-disclosure because of the possible information asymmetry value. This leads to:

Proposition 11: The less knowledge of privacy protection the employees of a Web site have, the lower disclosure rate of privacy protection practices the Web site has.

(12) Opinions from Other Decision-Making Participants

Some Web sites had departments of law. Those employees from the law department of the Web sites usually participated in reviewing their Web sites' policies and were supposed to resolve any disputes when necessary. Besides, as one of the Web site managers pointed out, many kinds of personnel are involved in the Web site design, including employees from MIS, law, marketing, and customer service departments, and even outside contractors. Therefore, others participating in disclosure decision-making process might have some degrees of influence. In other words, we postulate:

Proposition 12: Others participated in disclosure decision-making process, especially significant others, might have some influences on the disclosure of privacy protection practices.

(13) System Development Evolution Phase

The interviewed sites suggested that getting the consumers accustomed to the e-commerce mode over the Internet during the start-up stage should be far more important than considering the issues of on-line privacy. Therefore, in the early stage of system development, the issues of privacy disclosures might not be taken carefully.

From the view of information system design evolution, it would be natural that the functions of a start-up system were not comprehensive. Therefore, privacy disclosures would be considered as additional features, and would gradually be taken into account in a later stage. Especially, one site CEO emphasized the importance of Web design regarding product presentation and facilitating consumers' browsing convenience, rather than privacy disclosures. We thus state:

Proposition 13: The earlier phase the Web-site System Development lies in, the lower disclosure rate of privacy practices the Web site tends to have.

(14) Operational Benefits

According to our interviews, Web sites were inclined to disclose the information that could help foster transactions. It seems that the operational benefits had become a major factor in face of the trade-off of disclosures. This leads to:

Proposition 14: The higher the operational benefits that some information disclosure could bring, the more disclosures would happen.

(15) Gaps

As mentioned in section 7.1, the gaps between the intentions and actual performances, or between expectations and perceptions, lead to the inconsistency and the loss of customer confidence in the Web sites. Therefore, we postulate:

Proposition 15: The wider gaps a Web site has, the less consistent performance it has and the less confidence the Web users have in the Web site.

Possible Cultural Impacts on the Differences of Privacy Practices between the U.S. and Taiwan

In addition to the factors presented in the above model (Figure 3), the dimension of culture plays an important role in explaining the possible differences in privacy practices between the U.S. and Taiwan. As Lin and Tam (2000) suggested, the basic difference of privacy practices in different countries can be traced back to the differences in culture.

According to the culture theory of Hofstede (1980, 1991, 1997, 2000), national culture refers to "a collective programming of the mind which distinguishes one group from another." Hofstede identified five dimensions of national culture differences, each rooted in a basic problem with which all societies have to cope. These dimensions are *power distance*, *uncertainty avoidance*, *individualism versus collectivism*, *masculinity versus femininity*, and *long-term versus short-term orientation*. It can be conjectured that national culture might have certain impacts on a Web site operator's ethical decision and online marking strategy (Tsui and Windsor 2001; Simon 2001; Tian and Emery 2002). Therefore, because of different national cultures, the attitudes of top managers and other employees, as well as the whole organizational standpoint toward the

privacy-related matters might differ in different countries. This research has observed that privacy disclosures have become second citizens in designing Web systems in Taiwan, as compared to the U.S. In the following, we discuss the possible cultural impacts on Web site privacy practices.

(1) Power Distance

Power Distance refers to "the extent to which the less power members of institutions and organizations within a country that expect and accept power is distributed unequally" (Hofstede 1997). As Hofstede (1997, p.37) indicated, centralization is popular in the societies with large power distance. Traditionally, children in Taiwan have been trained to obey and the striving for personal rights is not normal. As a result, generally people is not accustomed to self-disclosing their own opinions, and then would not like to disclose customer rights to their customers as they become company mangers. Therefore, Web sites located in a country with a larger power distance like Taiwan might be more likely not to disclose their privacy policies.

In the cyberspace community of Taiwan, a Web site holds more power of information control than its users or customers. According to our survey, many Web sites did not allow customers to present their comments on products and services. Most of the Web sites in Taiwan do not allow Web users to opt-in or opt-out the future contact or the usage of personal information that might be beyond the scope of original purpose. Their consumers have less advantage. Once their rights were infringed, they might not be recovered. In general, the Web sites in Taiwan neglect to provide statements of contact channels for privacy concerns and complaint channels for privacy infringement.

(2) Uncertainty Avoidance

Uncertainty Avoidance refers to "the extent to which the members of a culture feel threatened by uncertain or unknown situations"(Hofstede 1997). It is the level of stress in a society in the face of an unknown future (Hofstede 2000). According to Hofstede (1997, p.113), Taiwan is a stronger uncertainty avoidance society, compared to USA. Taiwan is a densely populated island of limited land resources. People in Taiwan are accustomed to buying goods in traditional markets or other physical shops that involve face-to-face buying. They are less inclined to trust a "virtual" company on Web unless they have been already familiar with it. They are anxious about the safety and security of Web sites, especially those that are unheard of in the physical world. Therefore, security becomes one of the most important factors toward the Web site success. As found in this study, although the disclosure rate of security was low on average, the disclosure rate of the protective measures for data transmission (from client PC to Web server site) was still higher than other disclosure rates.

According to Hofstede (1997, p.125), a society with strong uncertainty avoidance has fear of ambiguous situations and unfamiliar risks. Therefore, the local and unfamiliar or unpopular seal programs were less convincing. In addition, the foreign authentication organizations have not yet become widely known to local inhabitants. This might explain that few privacy seals are found in the ".com.tw" or the ISP sites. On the contrary, users might be familiar with a Web site with excellent brand image. Therefore, a popular Web site might think its brand image would have more effect on customers' trust than privacy practice disclosure. However, it might not recognize that the disclosure privacy policies could further enhance their brand images.

As Hofstede (1997, p.122) indicated, weak uncertainty avoidance countries are more likely to stimulate basic innovations. On the contrary, a stronger uncertainty avoidance country has a higher tendency to suppress deviant ideas or even resist to innovation and is more likely to apply those innovations to develop pragmatic products (Hofstede, 1997, p.123). However, sometimes, the latter might just become a follower or a copier. This might explain why some Web sites located in Taiwan just copied other sites' business models and privacy policies to prevent the cost of try and error.

(3) Individualism versus Collectivism

Individualism refers to "societies in which the ties between individuals are loose"

and on the contrary, *collectivism* refers to "societies in which people from birth onwards are integrated into strong, cohesive in-groups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty"(Hofstede 1997). According to Hofstede, Taiwan is much more collectivist than USA. An individualist society has the fact that everyone has the right to privacy and is expected to have one's private opinion (Hofstede 1997, p.73). However, the concept of personal rights is not very rooted in the Taiwanese society, so that Web sites might be accustomed to neglecting customers' opinions. As a result, a Web site would not like to disclose its privacy policy and information practices, because it might assume that Web users waive their personal rights.

Even not to mention information privacy in the cyberspace community, the daily privacy issues are less important in Taiwan than in the U.S. and Europe. In Taiwan, an individual seldom complains of his (her) privacy infringement unless the resulting damage is significant enough for social attention. Therefore, organizations might not pay attentions to personal privacy issues.

(4) Masculinity versus Femininity

Masculinity pertains to "societies in which social gender roles are clearly distinct, (i.e., men are supposed to be assertive, tough, and focused on material success whereas women are supposed to be more modest, tender, and concerned with the quality of life); *femininity* pertains to societies in which social gender roles overlap, (i.e., both men and women are supposed to be modest, tender, and concerned with quality of life)"(Hofstede 1997).

According to Hofstede (1997, p.84), Taiwan is on the feminine side. However, Japan is a champion of masculinity, and USA is on the moderately masculine side. As Hofstede (1997, p.96) indicated, people and warm relationships are important in the feminine society. A society with low masculinity is relationship-oriented and a society with high masculinity is ego-oriented (Hofstede 2000, p.299). People in Taiwan like to build their interpersonal relationships. However, they might not build that kind of relationship with the Web sites which they have never known or seen their true faces, unless they use anonyms.

According to Tannen (1992), female discourse tends to use conversation to exchange feelings and establish relationships ("rapport talk") rather than transfer information ("report talk"). Therefore, shopping Web sites of Taiwan don't like to present their self-information, and prefer functionality design to plain-text form. As a result, the disclosure rate of privacy policy was low in general, because the policy usually looked like a "report"; and the disclosure rate of "notices" was low, since "notices" were generally presented in a plain-text form.

(5) Long-term versus Short-term Orientation

Long term orientation stands for "the fostering of virtues oriented towards future rewards, in particular perseverance and thrift; *short-term orientation* stands for the fostering of virtues related to the past and present, in particular respect for tradition, preservation of 'face', and fulfilling social obligations" (Hofstede 1997).

According to Hofstede(1997, 2000), Taiwan has a higher long-term orientation index value than USA. People in Taiwan have a virtue of thrift. They like to see and even try to touch real merchandise when shopping, and haggle over every penny to keep their spending down. This kind of culture might lead to less shopping in the Web sites. Besides, they value their personal relationship and also view it as an information source. They often judge things by referring to the members (such as relatives and friends) of their relationship networks. However, many web sites in Taiwan are just start-up, and might think that consumers would not appreciate the disclosures of privacy practices since they are new and have not gotten enough credibility yet. Therefore, these web sites doubted of the benefits that these disclosures could bring, and would rather devote their energy to marketing activities.

As Hofstede (2000, p.364) pointed out, people in East and Southeast Asia countries place less value on "cognitive consistency." People in Taiwan can adopt elements from different religions or adhere to more than one

religion at the same time. Hofstede (1997) believes that it is a type of Confucianism that becomes a cornerstone of society. On the other hand, they might be accustomed to having different meanings and treatments for a certain thing. For example, the content of disclosure might not be consistent with their mind or actual behavior. They even change their policies without giving customers notices once a certain circumstance changes. As a result, some discrepancies might happen among a Web site's decision outcome, actual disclosure, and actual behavior of privacy protection.

CONCLUSIONS

This study has examined the privacy practices of Web sites in Taiwan. This paper has discussed not only the differences between ISPs and non-ISP shopping Web sites, but also the differences between Taiwan and US Web sites. Moreover, by interviewing with Web site operators and introducing the culture theory of Hofstede (1980, 1991, 1997, 2000), we have explored possible disclosure determinants, presented some propositions, and discussed the possible impact of cultural differences on privacy practices.

As we all know, Web-site security, privacy protection, and open consumer contact and complaint channels are the basic criteria for building trust and relationship between Web sites and consumers. Trust is derived from establishment of a long-term relationship, and is an important means of enhancing customer loyalty. A Web site that does not possess the characteristics of a "safe harbor"[8] is unlikely to win customers' confidence.

However, in this study, we have found that despite the enormous popularity of the Internet applications, most Web sites in Taiwan did not post their privacy policies, nor did they comply with standards for transaction security. A great majority failed to adequately meet the requirements of the *Fair Information Practices*. Web-Wrap Agreements or on-line Click-Wrap Agreements[9] also tend to favor Web sites (Liu *et al.* 1998). This phenomenon seems inconsistent with the principles of reciprocity and good faith. Even the privacy disclosures of ISP sites, which kept a large number of real customers, did not fully satisfy customers who were concerned about personal privacy and transactional security.

The self-regulatory programs for information privacy in Taiwan are much more immature than those in the U.S. However, according to the research of the U.S. FTC (2000), even in the U.S., the actual effectiveness of calls made by self-regulatory programs was still limited. There is still room for improvement on such programs, which may be complemented by appropriate legislative measures. In fact, the secured environment of online privacy should be created by the collective efforts of government, industry, Web site operators, and consumers. Besides, as indicated by Barlow (1994), it is not sufficient to rely purely on legal protection. Ethics and the application of security technology are particularly important in this evolving e-net era. Therefore, in addition to mandatory legislation and industry self-regulation, self-governance is necessary for Web site operators to win consumer loyalty by enhancing their professional ethics and knowledge, as well as security and audit measures.

RECOMMENDATIONS

Following the Fair Information Practices and disclosing the privacy policy are just the minimum requirements for a Web site

[8] The "Safe Harbor" program is introduced at the request of the European Union. However, to April, 2001, only 37 US businesses have actually signed up with the Commerce Department's Safe Harbor program (C & M International 2001). Currently, there are 194 on the Safe Harbor List (U.S. Department of Commerce 2002).

[9] A "click-wrap agreement" is an agreement that sets forth the rights and obligations between parties, and is formed entirely in an online environment such as the Internet. Such an online agreement often requires clicking with a mouse on an on-screen icon or button to signal a party's acceptance of the contract.

to protect users' information privacy. Personal information privacy protection will depend on the soundness of government legislation and enforcement mechanisms, the Web site's professional ethics and management systems, as well as the monitoring by self-regulation bodies. The recommendations of this study are as follows:

About Government

- As a member of the global community, Taiwan has to conform to international standards. From the experiences of the U.S. and Europe, the government legislation efforts and industry self-regulatory efforts should be fully integrated.
- As mentioned in the section of literature review, although Taiwanese government has already enacted some laws and regulations for protection of privacy, such as the *Computer-Processed Data Protection Law*, it has not paid any attentions to the privacy disclosures of Web sites. Since the Internet is an international highway, some well-known local Web sites have already adopted the overseas practices of disclosing their privacy policies, but many Web sites still fail to do so. Government should encourage and even monitor their privacy disclosures. The privacy protection policies and legislations of international organizations or advanced countries (e.g., OECD, European Union, and U.S.) can be referenced. The research framework and questionnaire used in this study can also serve as a useful framework for the government when promoting privacy protection.
- The government should encourage industry bodies to address consumers' concerns regarding online privacy through self-regulation. Considering the balance among consumers' privacy, business freedom and technological advances, the government should wisely lead the Web sites to comply with self-regulatory program requirements.

About Web Sites

- A Web site should be aware of the importance of customers' concerns about security and privacy. The protection of customer information should be deemed as an effective means of enhancing customers' confidence or even as part of the Web site's competitive strategy.
- A Web site should provide proper disclosures of privacy policies regarding protection of personal information. To legitimize advertisement distribution, customers should be provided not only prior explicit consents but also options to cancel subscription later. After a Web user logs onto the sites, agrees its disclosures, makes or changes any privacy choice, the Web site should mail him/her a copy as a memo. In addition, Web sites should frequently review the disclosure contents to ensure that they conform to the current laws and social general expectations. In case of any necessary updates, Web sites should actively notify of their former customers. The Web disclosures should be carefully phrased to avoid misleading users. A feasible Web page design may look like the following: the fundamental or important disclosures are presented in a condensed manner shown at the top half of the screen, and detailed descriptions could be provided through hyper-linkages to a separate Web page or at the lower portion of the screen.
- A Web site should establish a comprehensive system to protect customer information. Such system should include education and training mechanisms to enable employees to learn legal knowledge, ethical judgment and technical know-how. Employees should sign confidential agreements and their awareness of customer's privacy should be reinforced. The internal information usage policy on a Web site should be formulated properly to win the trust of customers.

About Self-regulation

- The self-regulatory programs should be

focused not only on security, but also on privacy. This study found that in Taiwan less than 20% of Web sites possess a security seal (focusing on the data transmission security and transaction security), and less than 10% possess a privacy seal. The reasons for such phenomena might include the following: few famous local self-regulatory programs, the high costs of acquiring and maintaining a seal and so on. In fact, if the self-regulatory program is local, its acceptance by foreign users might become another issue.

- Users should be allowed to click a seal on a Web page to evaluate its privacy compliance.
- There were a lot of Web site competitions or evaluation activities held by industry or government in Taiwan. The evaluation criteria usually include popularity, Web page design factors, and transaction security, etc. However, the importance of privacy protection has not been recognized. The display of a privacy seal should be included in the evaluation criteria in the future.

LIMITATIONS AND FUTURE RESEARCH

Limitations

The model derived from the second phase of the study (as shown in Figure 3) has some limitations in generalizability. First, since the model was based on a handful of interviews, readers should be cautious if applying it to other cases. Second, the model has to introduce the national culture dimension as a moderating factor if applied to other countries, since all of the interviewed cases were local.

Future Research

Based on Figure 3, our future research will involve in-depth interviews of more Web site organizations, so as to understand their management states of privacy issues besides discovering the reasons behind the privacy policy disclosure. For example, is the collected personal information compiled to establish a profile of an individual's life? Is there detection and prompt rectification of errors in information? Are there considerations for long-term and short-term benefits for use of privacy information, and if so, how are these considerations made? Is customer privacy considered in terms of education, training, organizational structure or policy, and how is it ensured?

As mentioned in literature section, the US FTC has continued to concern about industry's effort on privacy protection by reviewing the privacy practices of US Web sites from year to year. Researchers or even Taiwanese authority might also continue to help industry development and enhance privacy protection by tracking the performance of Web-site privacy protection. In light of cultural differences (Hofstede, 1980, 1991, 1997, 2000; Vitell *et al.* 1993; Lin and Tam 2000; Husted 2000; Tsui and Windsor 2001; Simon 2001; Tian and Emery 2002) identified by this study, researchers might further study other privacy protection statuses, compare their differences and find better ways to promote the privacy protection and human rights.

ACKNOWLEDGEMENT

This study was sponsored by National Science Council, Taiwan (NSC 89-2416-H-004-093). Meanwhile, the authors would like to thank the senior editor and three anonymous reviewers for providing very valuable suggestions.

REFERENCES

Banisar, D., *Privacy & Human Rights 2000: An International Survey of Privacy Laws and Developments*, EPIC and Privacy International, 2000. Available at: http://www.privacyinternational.org/survey/index2000.html

Barlow, J. P., "The Economy of Ideas," March 1994. Available at: http://www.wired.com/wired/archive/2.03/economy.ideas.html

C & M International, *The Electronic Commerce Report*, The C & M International, April 12, 2001. Available at: http://www.crowell.com/worddocs/april2001.doc

Clarke, R., "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM,* 1999, 42, 60-67.

CFCT, *1999 ISP survey*, Consumers' Foundation, Chinese Taipei (CFCT), 1999. Available at: http://survey.yam.com/isp99/

Culnan, M., "Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission," June 1999a. Available at: http://www.msb.edu/faculty/culnanm/GIPPS/mmrpt.PDF

Culnan, M., "Privacy and the Top 100 Web sites: Report to the Federal Trade Commission," June 1999b. Available at: http://www.msb.edu/faculty/culnanm/GIPPS/oparpt.PDF

Culnan, M., "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing*; Spring 2000, 19:1, 20-26.

Federal Trade Commission (FTC), "Self-Regulation and Privacy Online," *A Federal Trade Commission Report To Congress*, July 1999.

Federal Trade Commission (FTC), "Privacy Online: Fair Information Practices in the Electronic Marketplace," *A Federal Trade Commission Report To Congress*, May 2000.

Givens, B., "A Review of State and Federal Privacy Laws," 1997. Available at: http://www.privacyrights.org/ar/jttaskap.htm

Greenleaf, G., "Global Protection of Privacy in Cyberspace - Implications for the Asia-Pacific," 1998. Available at: http://austlii.edu.au/itlaw/articles/TaiwanSTLC.html

Hofstede, G. H., *Culture's Consequences: International Differences in Work-Related Values*, CA: Sage Publications, 1980.

Hofstede, G. H., *Cultures and Organizations: Software of the Mind*, London: McGraw-Hill, 1991.

Hofstede, G. H., *Cultures and Organizations: Software of the Mind*, London: McGraw-Hill, 1997.

Hofstede, G. H., *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations,* 2nd Edition, CA: Sage Publications, 2000.

Husted, B.W., "The Impact of National Culture on Software Piracy," *Journal of Business Ethics*, August 2000, 26, 197-211.

Kramer, L.C., "Private Eyes Are Watching You: Consumer Online Privacy Protection-Lessons from Home and Abroad," *Texas International Law Journal*, Spring 2002, 37:2, 387-420.

Killingsworth, S., "Mining Your Own business: Privacy Policy in Principle and in Practice," *Journal of Internet Law*, October 1999, 1-18.

Lin, T.M. and J.C. Tam, "Personal Computer Data Privacy in Asia Pacific: Cross-Cultural Perspectives," *Journal of Computers*, 2000, 12:4, 45-59.

Liu, J.C., R.J. O'Connell, and W. S. Petty, "Electronic commerce: Using Clickwrap Agreements," *Computer Lawyer*, December 1998, 15, 10-17.

Liu, P., *Computer Law*, 2nd edition, Taipei: National Taiwan University Law School Press, 1988.

Microsoft, *Summary of Global Internet Legal Developments—from the Period October to December* 1999, Microsoft Corporation, 1999.

Milberg, S. J., S.J. Burke, H.J. Smith, and E. A. Kallman, "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM*, December 1995, 38:12, 65-74.

Morri, A. "Make it Click," *Telephony*, March 2, 1998.

Radcliff, D. "Is your ISP Secure?" *InfoWorld,* March 2, 1998.

Simon, S. J. "The impact of culture and gender on Web sites: An empirical study," *Database for Advances in Information Systems*, Winter 2001, 32:1, 18-37.

STLC, "Electronic Commerce on the Internet-Legal Developments in Taiwan," Science & Technology Law Center (STLC), 2002. Available at: http://stlc.iii.org.tw/earticles/EC-JM-U.htm#p6

Tannen, D. *You just don't Understand: Women and Men in Conversation*, London: Virage, 1992.

Tian, R.G. and C. Emery, "Cross-Cultural Issues in Internet Marketing," *Journal of American Academy of Business*, 2002, 1:2, 217-224.

Tsui, J. and Windsor C. "Some Cross-Cultural Evidence on Ethical Reasoning," *Journal of Business Ethics*, May 2001, 31:2, 143-150.

U.S. Department of Commerce, "Safe Harbor List," May 18, 2002. Available at: http://Web.ita.doc.gov/safeharbor/shlist.nsf/WebPages/safe+harbor+list, or http://www.export.gov/safeharbor/

Vitell, S.J., S.L. Nwachukwu, and J.H. Barnes, "The Effects of Culture on Ethical Decision-Making: An Application of Hofstede's Typology," *Journal of Business Ethics*, Oct 1993, 12:10, 753-760.

Wang, H., M. Lee, and C. Wang, "Consumer Privacy Concerns about Internet Marketing," *Communication of the ACM*, March 1998, 41: 3, 63-70.

Warren, S.D. and L.D. Brandeis, "The Right to Privacy," *Harvard Law Review*, 1890, 4, 193-220.

Westin, A., *Privacy and Freedom*, NY: Atheneum, 1967.

White & Case LLP, "*Global Privacy Law: A Survey of 15 Major Jurisdictions*," April 30, 2002. Available at: ttp://www.whitecase.com/report_global_privacy.pdf

AUTHORS

Heng-Li Yang is a professor in the Department of Management Information Systems, National Cheng-Chi University. His research interests include data & knowledge engineering, database and knowledge-based systems, software engineering, information management in organizations, privacy issues, technology impacts on organizations, electronic commerce and empirical studies in MIS. His articles have appeared in international journals such as *Information & Management*, *Journal Processing and Management*, *Cybernetics and Systems*, *Data and Knowledge Engineering, Expert Systems with Applications*, *Journal of Information Science and Engineering*, and *Industrial Management and Data Systems*.

Hsien-Kuei Chiu is a Ph.D. candidate in the Department of MIS at National Cheng-Chi University and a lecturer in the Department of MIS at Jin-Wen Institute of Technology. His current research interests include e-commerce, knowledge management, information technology management, and information ethics.