



Online Information Review

Privacy concerns, privacy practices and web site categories: Toward a situational paradigm

Chiung-wen (Julia) Hsu

Article information:

To cite this document:

Chiung-wen (Julia) Hsu, (2006), "Privacy concerns, privacy practices and web site categories", Online Information Review, Vol. 30 Iss 5 pp. 569 - 586

Permanent link to this document:

<http://dx.doi.org/10.1108/14684520610706433>

Downloaded on: 23 February 2015, At: 20:37 (PT)

References: this document contains references to 38 other documents.

To copy this document: permissions@emeraldinsight.com

The fulltext of this document has been downloaded 1642 times since 2006*

Users who downloaded this article also downloaded:

J. Alberto Castañeda, Francisco J. Montoso, Teodoro Luque, (2007), "The dimensionality of customer privacy concern on the internet", Online Information Review, Vol. 31 Iss 4 pp. 420-439 <http://dx.doi.org/10.1108/14684520710780395>

Jochen Wirtz, May O. Lwin, Jerome D. Williams, (2007), "Causes and consequences of consumer online privacy concern", International Journal of Service Industry Management, Vol. 18 Iss 4 pp. 326-348 <http://dx.doi.org/10.1108/09564230710778128>

S.E. Kruck, Danny Gottovi, Farideh Moghadami, Ralph Broom, Karen A. Forcht, (2002), "Protecting personal privacy on the Internet", Information Management & Computer Security, Vol. 10 Iss 2 pp. 77-84 <http://dx.doi.org/10.1108/09685220210424140>

Access to this document was granted through an Emerald subscription provided by 264686 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.



Privacy concerns, privacy practices and web site categories

Toward a situational paradigm

Toward a
situational
paradigm

569

Chiung-wen (Julia) Hsu

*Department of Radio and Television and Graduate Program,
College of Communication, National Chengchi University, Taipei, Taiwan*

Refereed article received
15 March 2006
Approved for publication
1 May 2006

Abstract

Purpose – The purpose of this research is to disprove the common assumptions of research into privacy concerns from an adversarial paradigm, which does not work in the context of the internet. These assumptions usually claim that internet users who have higher privacy concerns will disclose less information, and that data subjects are always adversarial to data users without considering social contexts.

Design/methodology/approach – The study surveyed 400 respondents from China, The Netherlands, Taiwan and the USA. It examined not only their privacy concerns, but also their actual practices, in order to identify any similarities between concerns and practices.

Findings – This study proved that internet users' privacy concerns do not reflect their privacy practices and showed how social contexts (Web category) influence users' privacy practices. Respondents from China, The Netherlands, Taiwan and the USA perceive Website categories in different ways, reflecting the influences of political systems, cultural background and economic development.

Research limitations/implications – This study maintains that future research on online privacy should take contexts or situations into account. To confirm this, additional research should be undertaken on how social contexts in other countries affect users' privacy concerns and practices. Investigators should also study what makes users more likely to disclose information.

Originality/value – This study suggests that legislation provides the basic protection, while self-regulation supplies the detailed principles of online privacy. Privacy education teaches users how to create their "zone of privacy" and how to be responsible for their online practices, in order to build an abuse-free information environment on the internet.

Keywords Privacy, Internet, China, The Netherlands, Taiwan, United States of America

Paper type Research paper

Introduction

Thousands of internet users post photos of themselves or their family on the internet (Spector, 2003), disclose information in return for discounts when ordering items on the internet, and disregard their anonymity when surfing on the internet. Does this mean that privacy is no longer important? This observation would seem to conflict with the findings of online privacy research. Is there anything wrong with the way in which online privacy is studied? This paper tries to resolve the fundamental problems which current privacy research tends to confuse or neglect – namely, social context, and differences between privacy concerns and actual practice.

First, privacy is dynamic rather than static. An individual might well have different privacy concerns in different situations. Privacy infringement is not always dangerous and people are not always adversely affected by privacy risks. Rather, there is a



Online Information Review
Vol. 30 No. 5, 2006
pp. 569-586

© Emerald Group Publishing Limited
1468-4527
DOI 10.1108/14684520610706433

difference of degree. Raab and Bennett (1998) are critical of the fact that scholars, when studying privacy, ignore the functional variety of data users and the sociological variables of data subjects. Instead, they concentrate on paying attention to how to stop data users from making use of data for surveillance and inappropriate business purposes, the adversarial paradigm. Raab and Bennett (1998) imply that people's privacy concerns vary when the situations and functions of data users change.

Second, privacy concerns do not parallel privacy practices. Most scholars assume that people's privacy concerns represent how they will behave when they encounter privacy risks. As a result, scholars usually ask about respondents' privacy concerns without double-checking respondents' actual practices.

There are many contexts which affect people's privacy concerns. This study focuses on the relationship between online privacy and Website category (context). Facing the challenge that privacy concerns do not parallel privacy practices and the awareness that Website categories influence internet users' privacy practices, this study suggests a situational paradigm to research privacy.

Literature review

The concept of privacy is complex. Privacy has broad historical roots in legal, political, philosophical, sociological and anthropological discussions. Researchers study what is privacy (the nature of privacy), the activities that infringe on privacy (privacy risks), how to protect privacy (privacy protection), and people's perception of privacy (privacy concerns). In the traditional adversarial paradigm, researchers display different views when discussing the nature of privacy; such views are mostly "the right to be let alone" (liberty) (Warren and Brandeis, 1890), "solitude" (Westin, 1968), "reserve" (Westin, 1968; Marshall, 1974; Pedersen, 1987), "anonymity" (Westin, 1968; Marshall, 1974; Pedersen, 1987), "intimacy" (Westin, 1968; Marshall, 1974; Rachels, 1975; Gerstein, 1978; Pedersen, 1987; Inness, 1992), psychological privacy/accessibility (autonomy) (Regan, 1995), and accessibility limited in certain contexts (secrecy) (Gavison, 1980; Allen, 1988). Researchers attempt to provide an exhaustive and complete definition of privacy, but never come to a definitive conclusion.

Following on from those fixed and incomplete concepts of privacy, some theories of privacy protection are developed. The four main theories – non-intrusion theory, seclusion theory, control theory and limitation theory – define privacy risks narrowly, and try to diminish the damage from them. However, it is not possible to control all risks in today's information society and no form of protection can cover all kinds of risks (Tavani, 1999). The major flaw in the current definition of privacy is that it assumes that people are vulnerable without considering the situational context, and as a result privacy risks are always deemed to be dangerous (Raab and Bennett, 1998).

Any study of the nature of privacy, privacy risks and privacy protection using the adversarial paradigm has to cope with new instances of privacy infringement. As Moor (1997) puts it, the privacy concept has been developed chronologically. In the current computer age, privacy has become very "informationally enriched". There is a need for an updated approach to studying privacy.

Moor identifies the problems and considers firstly "nature privacy and normative privacy" which challenges the assumption that people are vulnerable and provides a useful distinction between privacy right and privacy condition, and between a loss of privacy and an invasion of privacy. Second, he offers an alternative solution for

privacy protection - control/restricted access theory. In this centrist position “different people may be given different levels of access for different kinds of information at different times” (Moor, 1997).

Moor (1997) and Raab and Bennett (1998) propose moving the study of the nature of privacy, privacy risks, and privacy protection, from an adversarial paradigm towards a situational paradigm, especially in the context of the internet. However, it is clear that research into the study of privacy concerns, is still trapped in the adversarial paradigm.

At present studies into online privacy concerns tend to rely on an offline literature review, and try to discover what those using the internet think about privacy issues, by using demographics as independent variables. Some studies indicate that women tend to be more concerned about privacy than men (Kate, 1998; O’Neil, 2001). Internet users with higher levels of education are more concerned about their privacy than those with less education (Sheehan, 2002; O’Neil, 2001). Age, income, and technology demographics are also relevant to people’s privacy concerns (Milne and Rohm, 2000; Hoffman *et al.*, 1999).

However, the findings of research into privacy concerns based on demographics are usually conflicting. For instance, in contrast with the above research, the series of Equifax-Harris studies (Harris, 1990, 1995 quoted from Milne and Rohm, 2000) show that less affluent people are more concerned about threats to their personal privacy. As for age, Sheehan (2002) has different results, showing that people over the age of 45 years tend to be either not at all concerned about privacy or very concerned about privacy. The implication is that privacy concerns are not static but vary depending on the situation and context.

Contexts are not an original idea. Most research has been aware that understanding data subjects’ demographic variables is not sufficient to explain and predict data subjects. Contexts also determine subjects’ privacy practices and concerns. Hine and Eve (1998) raise the idea of situated privacy concerns by examining different situations qualitatively. They find that there is no particular kind of information that is always privacy sensitive in all kinds of contexts.

Lally (1996) provides quantitative evidence that situationally conditioned belief (SCB) makes the same individuals have a different belief, depending upon the situation in which they find themselves. According to Cho and LaRose (1999), consumers are willing to disclose their information based on the sensitivity of information and the intimacy of the relationship. If consumers know that the original Websites will transfer information to other types of companies without notice, they might not provide sensitive information, or refuse to give any information. This is consistent with the findings of Phelps *et al.* (2000).

Unlike the adversarial paradigm, researching privacy concerns needs to take two things into consideration. One is the context of privacy risks and data subjects; the other is a fundamental problem with studying privacy concerns. It is assumed that that people’s privacy concerns reflect their privacy practices. For example, if internet users have serious concerns about privacy risks, they will not give their information away. Is this true? In the ninth survey carried out by GVU (1998), 39.1 percent of respondents said that they are concerned about credit card security. According to O’Neil (2001), 78.7 percent of respondents claim that privacy is more important than convenience. It seems that privacy concerns dominate their online behaviors. However, when internet users

shop online, privacy concerns do not seem to be a primary concern. Bellman *et al.* (2000) found that privacy issues are not important predictors of buying versus not buying online.

This study argues that it is necessary to distinguish between privacy concerns and privacy practices. When researchers ask about internet users' online privacy concerns, respondents tend to think back to serious privacy infringements that they have experienced or heard about, and so rate their privacy concerns higher than their actual practice on the internet would suggest. However, when researchers ask about internet users' internet usage in the context of online privacy, users' daily practice tends to show that they might not be as concerned about privacy as seriously as their answers might suggest (GVU, 1998; Culnan and Armstrong, 1999).

As a result, in this study privacy concerns and privacy practices should be examined within the specific contexts of the data subjects. Contexts might be: technology (Sixsmith and Murray, 2001), Websites' performance (Hsu, 2002; Culnan and Armstrong, 1999), privacy regulations (Bennett, 1992), political system (Plichtova and Brozmanova, 1997), culture/country (Yamagishi and Yamagishi, 1994). In the adversarial paradigm, the country/culture variable is usually taken to equate with demographics. Research into privacy concern and privacy practice under a situational paradigm, revises the culture context of subjects as a social context along with social group.

Raab and Mason (2002) claim that people's concerns vary when the situation and function changes; put in the online context, the claim might be that Website categories influence internet users' privacy concerns and practices. When surfing commercial Websites, especially those involving online transactions, internet users worry about their credit card number being abused, but do they worry about giving away their address and real name? Without providing real name and address information, how can internet users receive the goods ordered on the internet?

Moreover, research increasingly notes the privacy problem of health Websites. When people search information about their health problem, they also disclose their health history, which can be transferred and combined and used in other ways, leading to job termination and the loss of insurance coverage (Graber *et al.*, 2002). Consequently, internet users might well be cautious when using health Websites.

The discussion above relates to the private sector. On the other hand, how do internet users perceive government Websites? In the USA, for example, there are few privacy laws regulating the private sector. This might be the reason that a "... self-help solution is of course very much in the American tradition, which dislikes paternalism and prefers to leave the citizen to pursue his rights through the courts" (Bennett, 1992, p. 199).

In most Asian countries democracy started in the twentieth century. People in those countries still maintain a totalitarian approach towards governments and as a result have little sense of privacy or surveillance (Fischer-Hübner, 1998). Do people from different countries have different attitudes toward the public sector?

Up to this point, this study has found that the current literature is problematic, and the adversarial paradigm fails to explain new phenomena. The solution may be a situational paradigm. Moor (1997), Tavani (1999), Raab and Bennett (1998), Lally (1996) and others support the same idea (see Table I). The purpose of this study is to find empirical evidence to support a situational paradigm by surveying internet users from the USA, The Netherlands, China and Taiwan.

	Adversarial paradigm	Situational paradigm
The nature of privacy	<ol style="list-style-type: none"> 1. Being let alone (Liberty) 2. Being alone (Solitude) 3. Psychological privacy/accessibility (autonomy) 4. Accessibility limited in certain context (secrecy) 	Natural and normative privacy
Privacy protection	<ol style="list-style-type: none"> 1. Non-intrusion theory 2. Seclusion theory 3. Control theory 4. Limitation theory 	Control/restricted access theory of privacy
Privacy risk	Data user v. data subject	<i>Contexts</i> Sectors (Website category) Technology/data
Privacy concerns	Data user v. data subject	<i>Privacy concerns/privacy practices</i> Individual contexts: demographics Social contexts: Culture Social group Policy regulations Space/place Websites' performance/category

Table I.
Two paradigms of
privacy research

Research questions and hypotheses

Following on from the previous discussion, research questions and hypotheses are formed as below.

Research questions

- RQ1.* What are the general privacy concerns and priorities in the USA, The Netherlands, China and Taiwan?
- RQ2.* What are the general privacy practices in the four countries?
- RQ3.* Do Website categories influence Internet users' willingness to give away information in each country respectively, and in all four countries?
- RQ4.* Do internet users disclose data at different frequencies for different types of information in different Website categories?
- RQ5.* How much do users' privacy concerns reflect their privacy practices?

Research hypothesis

- H1.* Country differences will be associated with differences in levels of privacy concerns.

Internet users from The Netherlands and the USA will be concerned about their general privacy more than those from China and Taiwan. But internet users from China and Taiwan will be concerned more about their in-group privacy than those in The Netherlands and the USA. In line with Taylor *et al.*'s (2000) investigation, USA consumers would be expected to express more concern about mailing list rental issues than Japanese consumers. The Japanese, in contrast, are more concerned about differentiating between people "inside" and "outside" their "private world" (*uchi*). In other words, people from Asia seem to care more about their in-group privacy.

As for the differences between the USA and The Netherlands, users from The Netherlands, where there is more emphasis on stricter regulation and privacy being perceived as a human right, might be concerned more about privacy. And as for the differences between China and Taiwan, internet users from China seem to have fewer privacy rights in their daily lives and, consequently, they might have fewer privacy concerns than users from Taiwan.

H2. Country differences will be associated with differences in levels of privacy practices.

Internet users in The Netherlands release less information than those in the USA. Internet users in China release more information than those in Taiwan:

H3. Higher levels of privacy concerns will result in smaller amounts of information being released (privacy practices).

Methodology

Instrument construction

Users are asked to disclose personal information according to a specific Website's requirements. The scope of personal information in this study followed the "most frequently asked information" lists developed by the Georgia Institute of Technology GVU (1998) together with "sensitive" information, as emphasized by privacy advocates. To sum up, personal information is any information that can be attributed to individual users, including name, address, email address, telephone number(s), names of family members, ID card number(s) or credit card number(s), financial information and medical history.

Instead of asking how much users are concerned about disclosing their personal information, this study asks how often users provide personal information to understand the real practices of their disclosure behaviors, not their concerns. The questionnaire asked users about their willingness to release information in five different categories, including government Websites, commercial Websites, health Websites, non-profit Websites, and community Websites.

Government Websites represent the public sector; commercial Websites represent the private sector; the non-profit Websites represent those third parties which are neither public nor private sectors, such as advocate groups, university, and charity groups. Community Websites can also be partly private, but the main function is to provide a platform in order to provide Internet users with free email services, free Web spaces, online chatting rooms, online discussion groups and search engines. Frequency of use was indicated on a 7-point Likert scale (1) "never" to (7) "always", with a "don't know" option. The privacy concerns questionnaire is adapted from previous research (Smith *et al.*, 1996).

Data collection

The total sample for this study is drawn from 400 volunteers from urban universities in China, The Netherlands, Taiwan, and the USA. 100 students from each country answered the survey by means of a Web questionnaire. Use of student subjects always brings issues of generalization. While student samples may not be ideal, students are routinely used in this cross-country research. However, there is also some advantage in using students as subjects. In this research, education and vocation are controlled, from which parsimony theory building benefits in this early stage.

Results

General privacy concerns and priorities

In order to answer *RQ1* and *H1*, *t* test with LSD is performed. All 15 questions are added as total privacy concerns. The mean of Taiwanese respondents is significantly higher than those in the other three countries. The USA ranks lowest in terms of privacy concerns (see Table II).

H1 partly maintains and partly rejects the hypothesis. The Dutch and US respondents do not worry about their general privacy more than those from China and Taiwan. Results show that both Chinese and Taiwanese respondents worry more about improper data sharing and usage, which could be seen as in-group privacy, since they only want to share their information with the original Websites. Of US and Dutch priorities, data error is the most important issue.

General privacy practices

RQ2 wants to know about the general privacy practices in the four countries. The study combined all the information types in each Website category and obtained the mean. It then summed up all the mean figures of practices from five Website categories, to obtain a general privacy practices mean from each country. Judging from the results, Chinese and Taiwanese respondents release more information to Websites than Dutch and USA respondents (see Table III). This answer also proved the truth of *H2*: internet users in The Netherlands release less information than those in the USA; internet users in China release more information than those in Taiwan.

	USA	Netherlands	China	Taiwan
Total privacy concerns mean	5,439	5,652	5,667	6,356
<i>F</i> (sig.)	20,78 (0.000)			
LSD	U-T	D-T	C-T	T-U, T-D, T-C

Table II.
General privacy concerns
of the four countries

USA	Netherlands	China	Taiwan	<i>F</i> (sig.)	LSD	Order
2,2731	2,2417	2,9827	2,8996	17,134 (0.000)	C-D, U D-T T-U	CT-UD

Table III.
General privacy practices
of the four countries

OIR
30,5

576

Website categories and privacy practices

To answer *RQ3*, the study combined all the information types' disclosure in each Website category and obtained the mean, called the total privacy practices mean, within one Web category. It then compared the total privacy practices means respectively with government, commercial, health, non-profit and community Web categories. The multiple analysis of variance (MANOVA) for dependent sample was employed (see Table IV).

The US respondents were found to be disclosing more information to commercial Websites, and then non-profit, government, community and health Websites in descending order. The Dutch respondents disclose more to the government and commercial Websites, and then health, non-profit and community Websites. For Chinese respondents, government Websites and community Websites are the Website categories to which the Chinese respondents disclose more about themselves. The second Web categories are both non-profit, and commercial Websites. Health Websites are the most sensitive. The ascending order of Taiwanese respondents is government and commercial, community and health, and non-profit Websites. Government and commercial Websites are both less sensitive.

The following comparison is to see how the respondents from four countries perceive the five Website categories when disclosing their information (see Table V). Overall, ANOVA results shows that total privacy practices of the USA, The Netherlands, China and Taiwan in five Web categories are all significantly different. Government ($F = 33.370$) and community ($F = 37.393$) Websites have greater variances. In the government Web category, the Chinese and Taiwanese respondents disclose more than their two counterparts. The US respondents are reluctant to give their information to government Websites. The Asian countries are recognized as more obedient to governments than the western countries. This proved that different countries might have different perceptions regarding the public sector, which also works in the Internet setting.

The other category is community Websites. In some cross-cultural research, scholars claim that Asian countries do not care about individual privacy as much as their counterparts, but that they care more about their in-group privacy. The ANOVA result shows that the Chinese and Taiwanese respondents are more willing to give away their privacy to community Websites than the US and Dutch ones. The Chinese respondents' privacy practices are even liberal more than the Taiwanese. This implies

Table IV.
The MANOVA
comparison of total
privacy practices means
within one Web category
(within one country)

	USA	Netherlands	China	Taiwan
Government (G)	2.238	2.631	3.323	3.295
Commercial (C)	2.916	2.578	2.782	3.226
Health (H)	1.837	2.083	2.675	2.677
Non-profit (N)	2.413	2.022	2.840	2.496
Community (M)	1.962	1.894	3.293	2.804
F (sig.)	12.52 (0.000)	24.04 (0.000)	18.49 (0.000)	16.19 (0.000)
Pair samples	G-C, H, N, M	G-H, N, M	G-C, H, N	G-H, N, M
t test	C-H, N, M	C-H, N, M	C-H, M	C-H, N, M
	H-N, M	N-M	H-M	N-M
	N-M		N-M	
Descending	C-N-G-M-H	GC-HN-M	GM-NC-H	GC-MHN

Table V.
The ONE-WAY ANOVA
comparison of total
privacy practices means
within one Web category
among the four countries

	USA	Netherlands	China	Taiwan	<i>F</i> (0.000)	LSD	Descending order
Government	2.2857	2.6044	3.4090	3.2773	33.370 (0.000)	C-D, U D-T T-U	CT-DU
Commercial	2.9755	2.5480	2.9293	3.3829	10.944 (0.000)	C-D, T D-U T-D, U	T-U-C-D
Health	1.9393	2.1167	2.6406	2.7556	10.590 (0.000)	C-D, U D-T T-U	TC-D-U
Non-profit	2.5976	2.0792	3.0632	2.4838	12.989 (0.000)	C-D, T D-T, U T-U U-C	C-U-T-D
Community	2.2191	1.9365	3.3542	2.9934	37.393 (0.000)	C-D, T D-T T-U U-C	C-T-UD

that they share more information within a group and are less concerned about their individual privacy.

In the commercial Web category, the descending order is Taiwan, the USA, China and The Netherlands. Usually, the Taiwanese and Chinese respondents disclose more. But the US respondents' privacy practices in this category are apparently increasing, putting them second position. This is in accordance with the US data protection status quo. The USA tends to trust the private sector more than the public one. In health Web categories, the respondents from four countries simultaneously reduced the amount of information they disclose. This shows that genetic information is very sensitive regardless of country.

The non-profit Web category is a very interesting one. The Chinese respondents tend to regard them as parallel to the government Websites. The Dutch and Taiwanese respondents seem to regard them as sensitively as health Websites. The US respondents think it is similar to commercial Websites. Thus, it is necessary to investigate the non-profit Websites' operation amongst the four countries for more explanation.

Website categories and information types

RQ4 would like to know if the different types of information would be disclosed differently based upon the Website categories within one country. The MANOVA for a dependent sample was adopted.

The US respondents (see Table VI) give more demographic information to commercial Websites, and then government, non-profit and community Websites. They give less demographics to health Websites. Identification card number is considered somewhat sensitive information, for respondents. The US respondents disclose ID numbers more to non-profit Websites and then commercial Websites. The least disclosure is still to health Websites. Interestingly, the same Website category does not

OIR
30,5

578

	G	C	H	N	M	<i>F</i> (sig.)	Pair samples <i>t</i> test	Descending order
Demographics	3.810	4.190	2.276	3.379	3.017	13.93 (0.000)	G-C, H, M C-H, N, M H-N, M	C-GNM-H
ID card	1.828	2.086	1.603	2.931	1.534	10.85 (0.000)	G-C, N C-N, M H-N N-M	N-C-GMH
Credit card	1.667	3.281	1.491	1.807	1.491	20.95 (0.000)	C-G, H, N M	C-NGMH
Contact	2.536	3.804	1.821	3.250	2.304	15.53 (0.000)	G-C, N C-H, M H-N N-M	CN-GMH
Online contact	3.714	4.429	2.625	3.768	3.375	10.73 (0.000)	G-C, H, M C-H, N, M H-N, M	C-NG-M-H
Consumer history	2.130	2.648	1.537	1.574	1.444	14.05 (0.000)	G-C, N, M C-H, N, M H-G, N, M N-M	C-G-N-H-M
Health history	1.393	1.429	2.054	1.464	1.286	6.26 (0.000)	G-H C-H H-N, M	H-NCGM
Other family members' info	1.368	1.632	1.421	1.526	1.421	0.91 (0.456)		

Table VI.
The MANOVA
comparison of eight types
of information and
Website categories from
the USA

always have the same degree of user disclosure. For example, the respondents are not willing to give their ID number to government Websites even though they are happy to disclose their demographic information. Credit card number is one of the categories of information causing most concern within this dataset. Respondents do not disclose a lot of their information, except to commercial Websites. They would not like to give their ID number to commercial Websites but are more often prepared to give their credit card numbers. This is logical since if users are going to buy, sell or auction off some products from the internet, they have to disclose their credit card number.

Compared to demographics, contact information is still somewhat sensitive. Again, the US respondents reveal more of their contact information to commercial and non-profit Websites and less to government, community and health Websites.

Online contact information is the least sensitive information among the eight types. The descending order is commercial, non-profit and government, community, and health Websites. The last Website categories to which respondents will give their consumer history are community and health.

Health information and other family members' information are the two most sensitive types of information. The US respondents tend to give more health history to health Websites. Apart from this, no matter what Website category respondents visit, they seldom disclose these two types of information.

The Dutch respondents (see Table VII) like the US respondents, regard demographics and online contact information as the types of information causing the least concern. The Dutch respondents disclose more demographic and online contact information to government and commercial Websites and then health, non-profit and community Websites. Contact information and consumer history are close in terms of disclosure frequency. The Dutch respondents reveal more contact information to government and commercial Web categories, and then non-profit, health and community Websites. ID number, credit card number, health history and other family members' information are the least disclosed information types. Website categories, according to descending order of disclosure of ID number, are commercial, government, health, non-profit and community. There is a similar order for disclosure of credit card number. The Dutch respondents also seldom make public their health history. They disclose more health history to health Websites, and then government and commercial, non-profit and community Websites. Other family members' information is very sensitive regardless of the Website categories.

Health and government Websites do not cause as much concern as those in the USA; instead, the community Websites cause the most concern. Community Websites are always the least likely to generate disclosure of information, no matter what type of information.

The Chinese respondents disclose online contact information more than any other type of information (see Table VIII). They disclose more to community Websites, and then to government, non-profit and commercial Websites. The least information was disclosed to health Websites. Demographics as much as online contact information are often revealed more than other information. For the US and Dutch respondents, ID number is almost as important as credit card number. But the Chinese respondents reveal more ID card numbers than credit card numbers, especially to government

	G	C	H	N	M	<i>F</i> (sig.)	Pair samples <i>t</i> test	Descending order
Demographics	4.417	4.417	3.375	3.167	3.000	15.83 (0.000)	G-H, N, M C-H, N, M	CG-HNM
ID card	1.204	1.265	1.184	1.163	1.143	2.00 (0.096)	G-N C-N, M	CGHNM
Credit card	1.429	1.571	1.143	1.245	1.122	7.28 (0.000)	G-C, H, N, M C-H, N, M	C-G-NHM
Contact	3.327	3.245	2.673	2.714	2.286	10.90 (0.000)	G-H, M C-H, N, M H-M N-M	GC-NH-M
Online contact	4.714	4.490	3.449	3.408	3.224	19.47 (0.000)	G-C, H, N, M C-H, N, M	GC-HNM
Consumer history	3.326	3.196	2.348	2.283	2.087	17.24 (0.000)	G-H, N, M C-H, N, M H-M	GC-HNM
Health history	1.347	1.204	1.510	1.020	1.020	5.20 (0.000)	G-H, N, M C-H, N, M H-N, M	H-GC-NM
Other family members' info	1.163	1.061	1.082	1.122	1.041	1.36 (0.250)		

Table VII.
The MANOVA
comparison of eight types
of information and
Website categories from
The Netherlands

OIR
30,5

580

Table VIII.
The MANOVA
comparison of eight types
of information and
Website categories from
China

	G	C	H	N	M	F (sig.)	Pair samples <i>t</i> test	Descending order
Demographics	4.573	3.933	3.733	3.987	4.747	13.90 (0.000)	G-C, H, N C-M H-M, N-M	MG-NCH
ID card	3.667	2.733	2.733	3.267	3.587	15.81 (0.000)	G-C, H, N C-N, M H-N, M	GMN-HC
Credit card	1.827	1.827	1.507	1.640	1.853	2.75 (0.028)	G- H, N C-H N-M	MGCNH
Contact	3.405	3.165	2.848	3.443	3.785	7.71 (0.000)	G-H, M C-H, N, M H-N, M N-M	M-NGC-H
Online contact	5.101	4.392	4.025	4.456	5.354	25.69 (0.000)	G-C, H, N, M C-H, M H-N, M N-M	M-G-NC-H
Consumer history	4.200	3.400	2.973	2.867	3.893	14.46 (0.000)	G-C, H, N C-H, N H-M N-M	GMC-HN
Health history	2.293	1.707	2.253	1.800	1.800	10.37 (0.000)	G-C, N, M C-H, N H-N, M	GH-NMC
Other family members' info	1.707	1.333	1.600	1.480	1.480	4.43 (0.002)	G-C, M C-H, N	GHNMC

Websites. Information is disclosed least to health and commercial Websites. As for contact information, they give more to community Websites, and then non-profit, government, commercial and health Websites.

Consumer history for the Chinese subjects seems to be the same as ID number. They disclose more to government and community Websites. They tend to give a lot of information to community Websites, except health history and other family members' information. These two types of information are revealed more to government and health Websites. Ironically, the health Website is often taken as a more worrying Web category. But the Chinese respondents give the most sensitive information to this Web category. It is necessary to check if the health Websites usually ask for family health history in order to give services.

The Taiwanese respondents' most frequently disclosed information types are demographics and online contact information (see Table IX). They tend to disclose these types of information more to government, commercial and community Websites, and less to health and non-profit Web categories. Like the Chinese respondents, ID number is not as important as credit card number. However, Taiwanese respondents seem to trust commercial Websites more than their Chinese counterparts.

	G	C	H	N	M	<i>F</i> (sig.)	Pair samples <i>t</i> test	Descending order
Demographics	4.733	4.583	3.900	3.800	4.483	6.82 (0.000)	G-H, N C-H, N H-M N-M	GCM-HN
ID card	3.400	3.433	2.700	2.433	2.933	8.88 (0.000)	G-H, N C-H, N, M N-M	CGMHN
Credit card	1.483	1.817	1.350	1.483	1.367	3.61 (0.007)	G-C C-H, N, M	C-GNMH
Contact	3.721	3.918	3.180	3.082	3.672	6.77 (0.000)	G-C, H, N C-H, N, M H-M N-M	C-GM-HN
Online contact	4.836	4.885	3.869	3.918	4.574	10.15 (0.000)	G-H, N C-H, N H-M N-M	CGM-NH
Consumer history	4.117	3.933	2.633	2.400	2.600	34.66 (0.000)	G-H, N, M C-H, N, M N-M	GC-HM-N

Table IX.
The MANOVA
comparison of eight types
of information and
Website categories from
Taiwan

Credit card number is the most sensitive information type for the Taiwanese respondents. They disclose more to commercial, government and non-profit Web categories. Contact information is somewhat more sensitive than online contact information, which is revealed more to commercial, government and community Websites. Consumer history is almost the same as ID number; however, the Taiwanese disclose this type of information to government and commercial Websites far more than any other three. Other family members' information is disclosed less. In general, the Taiwanese subjects disclose more to commercial and government Web categories.

Privacy concerns are not parallel to privacy practices

RQ5 is related with *H2* and is answered by respondents' self-report of attitude and behaviour towards privacy. ANOVA shows there is slight significant difference between these two variables (see Table X). But the regression result shows the interrelationship is almost none. *t*-value and *F* value are not significant at all. The explained variance is lower than 0.1 per cent (see Table XI). *H3* is rejected.

Discussion

In order to connect the statistical results with the real world, the bias of the sample has to be more clearly articulated. First, students are experienced internet users and have internet access at least through their school. Secondly, in this study, the response rate is unknown. Therefore, the results may under-report or over-report those internet users' privacy concerns and privacy practices. Research bias might exist in either way.

Research findings mostly support the two main arguments of this research, except that respondents of the two Asian samples are found to be concerned more about privacy than those of the two Western countries. Sample bias might be one of the

reasons. Additionally, it is necessary to cross-examine privacy concerns with the influences of internet experience and the prosperity of online business.

However, the same Chinese and Taiwanese respondents are found to disclose information more than the US and Dutch respondents. It is proved that there is little relationship between privacy concern and privacy practices. And it confirms another main argument that data subjects (Internet users) are not always adversarial to data users (Websites) but act according to the contexts.

The same Website category is perceived differently amongst the four countries. Government Websites are seen as sensitive Websites by the US respondents, who disclose less information. However, the two Asian counties trust government Websites more than others, in accordance with the findings of Fischer-Hübner (1998). Dutch respondents also take government Websites as less sensitive and give a bit more information.

As for commercial Websites, the US respondents disclose far more information to them than other categories. Nevertheless, the Chinese respondents tend to give less information to commercial Websites. In addition, the community Websites seem to be more credible for the Chinese and Taiwanese respondents but not for the USA and Dutch.

Comparing the US respondents with the Dutch, although the two Western countries have similar political systems, the Dutch respondents tend to disclose more information to government Websites, and commercial Websites are the second most frequently disclosed Website category, which is opposite to the US respondents. Government Websites are the third Website category in terms of disclosing frequency lower than non-profit Websites. It seems that cultural background plays an important role in differentiating between these two countries.

As for the Taiwanese and Chinese respondents, commercial Websites seem to be more sensitive to the Chinese respondents than the Taiwanese. The development of e-commerce might be a crucial factor. Generally speaking, all respondents disclose significantly less information to health Websites.

Some research has found that some information is more sensitive than other types, such as ID number and credit card number. This study argues that so-called sensitive

Table X.
Effects of privacy
concerns on privacy
practices

	Sum of squares	df	Mean square	<i>F</i>	Sig.
Between groups	104.440	82	1.274	2.662	0.000
Within groups	61.725	129	0.478		
Total	166.165	211			

Table XI.
Regression of privacy
concerns for privacy
practices

Independent variable	Standardized coefficients
Privacy concerns	0.023 (0.330 ^a)
Number of observation	212
<i>R</i> square	0.001
<i>F</i> value	0.109
Note: ^a <i>t</i> ratio	

information is not always sensitive. For those who would like to buy products from the Internet, a credit card number and contact information are needed.

Health history is an extremely sensitive information type. The Chinese and Taiwanese respondents both give the most sensitive information, “other family members’ information” to the most sensitive Websites, health Websites. Why? It might be because health Websites sometimes ask for family disease background. It is reasonable for them to give health history to health Websites in order to get some useful medical information. However, it would be odd to give health history to community Websites. As a rule, people tend to give the information type which is necessary for the specific Website category.

Based upon the above discussion, we can see that contexts control internet users’ behaviour more than demographics. However, this is something beyond the scope of this research. It is not certain if the same situation has occurred in other user samples. The student samples are experienced internet users who are capable of judging which information type the Website needed. They are also able to tell what Website categories might lead to more risks if they disclose their information. Therefore, there are some limitations needing clarification in future research.

Policy implication

In verifying the two fundamental problems of privacy concerns research, this study gives the indicators to policy-making and information gathering, storage, and retrieval, by Websites. At the macro level, the respondents from four countries have different priorities, privacy concerns and privacy practices regarding Website categories. It implies that there is no standard definition of privacy (global privacy) and privacy protection, which could be suitable for every country. Policy makers have to recognize the differences of country/culture, technology, regulation, and so on. It does not mean we do not need any global protection guidelines. Fair information principles, such as the OECD guidelines and Safe Harbor Privacy Principles, are essential to give the basic protections. Further, the international differences in information privacy call attention to a need for local considerations (Ribak and Turow, 2003). The minimum protection of personal data protection including notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress should be implemented by legislation.

After fulfilling basic fair information principles, the next step is to take contexts (Website categories) into consideration to somehow amalgamate comprehensive principles. Self-regulation is a more appropriate mechanism for focusing on the details of compliance, standardization and consequence based upon contextual differences, such as Website category and information types. Unlike regulatory authority, self-regulation quickly adjusts the changing technology and provides prompt and detailed guidelines for data users with adequate levels of standardization and non-compliance penalties.

At the micro level, this study introduces Moor’s (1997) “zones of privacy” for solutions of possible privacy infringements caused by reckless internet users. A zone of privacy is a set of privacy situations in which people become aware of aspects of their personal information that may be damaging to them if made public. In the internet setting, with different zones of privacy, individuals can judge what type and how much information to keep private and which to make public. Following this logic, a

combination of privacy and technology education is suggested to assure privacy protection for Internet users. Privacy education should be taught not only in school, but also in the community and society by means of the media and reports. With basic know-how of online privacy, internet users need to learn possible consequences and take more responsibility for their information disclosure.

Recommendation

It is necessary to survey more internet users randomly. Future research needs to recognize the difference between privacy concerns and privacy practices. In this study, most privacy practices are obtained from users' self-administered reports. It is possible that respondents either overestimate or underestimate their daily usage. The alternative for future research is to use computer software to monitor users' daily usage.

Numerous variables have been uncovered in this investigation. From the literature review it is apparent that both technology and the physical environment might influence internet users. Some scholars find that using the internet at home or at work leads to different surfing patterns (Miller and Weckert, 2000). Another consideration is whether users share a computer with other family members or have their own. Does it influence their privacy practices on the internet too? It is therefore crucial to find more contexts which are able to predict internet users' behaviour on the internet.

The predictive power of Website categories is to some extent proved in this research. The next step is to examine further why some Website categories are trusted by internet users and some are not. What are the differences between countries? After finding the contexts which are able to predict internet users' behaviour, the next step is to use structural equation models (SEM) such as LISREL to confirm the cause-effect relationship.

References

- Allen, A. (1988), *Uneasy Access: Privacy for Women in a Free Society*, Rowman and Littlefield, Totowa, NJ.
- Bellman, S., Lohse, G.L. and Johnson, E.J. (2000), "Predictors of online buying behavior", *Communications of the ACM*, Vol. 42 No. 3.
- Bennett, C.J. (1992), *Regulating Privacy*, Cornell University Press, Ithaca, NY.
- Cho, H. and LaRose, R. (1999), "Privacy issues in Internet surveys", *Social Science Computer Review*, Vol. 17 No. 4, pp. 421-34.
- Culnan, M. and Armstrong, P. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: an empirical evidence", *Organization Science*, Vol. 10 No. 1, pp. 104-15.
- Fischer-Hübner, S. (1998), "Privacy and security at risk in the global information society", *Information, Communication & Society*, Vol. 1 No. 4, pp. 420-41.
- Gavison, R. (1980), "Privacy and the limits of the law", *Yale Law Journal*, Vol. 89, pp. 421-71.
- Gerstein, R. (1978), "Intimacy and privacy", *Ethics*, Vol. 89, pp. 76-81.
- Graber, M.A., D'Alessandro, D.M. and Johnson-West, J. (2002), "Reading level of privacy policies on internet health Websites", *The Journal of Family Practice*, Vol. 51 No. 7, pp. 642-5.
- GVU (1998), Georgia Institute of Technology, Gvu "Ninth WWW user survey".
- Hine, C. and Eve, J. (1998), "Privacy in the marketplace", *Information Society*, Vol. 14 No. 4, pp. 253-62.

- Hoffman, D.L., Novak, T.P. and Peralta, M.A. (1999), "Information privacy in the marketplace: implications for the commercial uses of anonymity on the Web", *Information Society*, Vol. 15 No. 2, pp. 129-39.
- Hsu, C.W. (2002), "Online privacy issues: comparison between net users' concerns and Websites' privacy statements", *Proceedings of the 52nd Annual Conference of International Communication Association, Seoul, Korea*.
- Inness, J. (1992), *Privacy, Intimacy and Isolation*, Oxford University Press, Oxford.
- Kate, N. (1998), "Women want privacy", *American Demographics*, Vol. 20 No. 1, p. 37.
- Lally, L. (1996), "Privacy versus accessibility: the impact of situationally conditioned belief", *Journal of Business Ethics*, Vol. 15, pp. 1221-6.
- Marshall, N.J. (1974), "Dimensions of privacy preferences", *Multivariate Behavioral Research*, Vol. 9, pp. 255-72.
- Miller, S. and Weckert, J. (2000), "Privacy, the workplace and the internet", *Journal of Business Ethics*, Vol. 28 No. 3, pp. 255-65.
- Milne, G.R. and Rohm, A.J. (2000), "Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives", *Journal of Public Policy & Marketing*, Vol. 19 No. 2, pp. 238-49.
- Moor, J.H. (1997), "Towards a theory of privacy in the information age", *Computers and Society*, Vol. 27 No. 3, pp. 27-32.
- O'Neil, D. (2001), "Analysis of Internet users' level of online privacy concerns", *Social Science Computer Review*, Vol. 19 No. 1, pp. 17-31.
- Pedersen, D.M. (1987), "Sex differences in privacy preferences", *Perceptual and Motor Skills*, Vol. 48, pp. 12139-42.
- Phelps, J., Nowak, G. and Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 27-41.
- Plichtova, J. and Brozmanova, E. (1997), "Social representations of the individual and the community well-being: comparison of the empirical data from 1993 and 1995", *Sociologia*, Vol. 29 No. 4, pp. 375-404.
- Raab, C.D. and Bennett, C.J. (1998), "The distribution of privacy risks: who needs protection", *The Information Society*, Vol. 14, pp. 263-74.
- Raab, C.D. and Mason, D. (2002), "Privacy, surveillance, trust and regulation: a series, Information", *Communication & Society*, Vol. 5 No. 2, pp. 237-41.
- Regan, P.M. (1995), *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, NC.
- Rachels, J. (1975), "Why privacy is important", *Philosophy and Public Affairs*, Vol. 4, pp. 323-33.
- Ribak, R. and Turow, J. (2003), "Internet power and social context: a globalization approach to Web privacy concerns", *Journal of Broadcasting and Electronic Media*, Vol. 47 No. 3, pp. 328-49.
- Sheehan, K.B. (2002), "Toward a typology of internet users and online privacy concerns", *The Information Society*, Vol. 18, pp. 21-32.
- Sixsmith, J. and Murray, C.D. (2001), "Ethical issues in the documentary data analysis of internet posts and archives", *Qualitative Health Research*, Vol. 11 No. 3, pp. 423-32.
- Smith, H.J., Milburg, S.J. and Burke, S.J. (1996), "Privacy, surveillance, trust and regulation: a series, Information", *MIS Quarterly*, Vol. 20 No. 2, pp. 167-96.

-
- Spector, L. (2003), "Guide to Online photo album sites: here's how to post and share digital memories of your holidays", *PC World*, December, p. 26.
- Tavani, H.T. (1999), "Privacy online", *Computers and Society*, Vol. 29 No. 4, pp. 11-19.
- Taylor, C.R., Franke, G.R. and Marynard, M.L. (2000), "Attitudes toward direct marketing and its regulation: a comparison of the United States and Japan", *Journal of Public Policy & Marketing*, Vol. 19 No. 2, pp. 228-37.
- Warren, S. and Brandeis, L. (1890), "The right to privacy", *Harvard Law Review*, Vol. 4 No. 5, pp. 193-220.
- Westin, A. (1968), *Privacy and Freedom*, Atheneum, New York, NY.
- Yamagishi, T. and Yamagishi, M. (1994), "Trust and commitment in the United States and Japan", *Motivation and Emotion*, Vol. 18, pp. 129-66.

Corresponding author:

Chiung-wen (Julia) Hsu can be contacted at: juliachiung@yahoo.com

This article has been cited by:

1. Horst Treiblmaier, Sandy Chong. 2013. Trust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure. *Journal of Global Information Management* **19**:10.4018/JGIM.20111001, 76-94. [[CrossRef](#)]
2. Trina J. Magi. 2011. Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature 1. *The Library Quarterly* **81**, 187-209. [[CrossRef](#)]
3. Alireza Chavosh. 2011. Comparing the Satisfaction with the Banks E-payment Services between Degree Holder and Non-Degree Holder Customers in Penang-Malaysia. *International Journal of e-Education, e-Business, e-Management and e-Learning* . [[CrossRef](#)]
4. Cho Hichang. 2010. Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies. *Journal of Information Privacy and Security* **6**, 3-27. [[CrossRef](#)]
5. Jiunn-Woei Lian, Tzu-Ming Lin. 2008. Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior* **24**, 48-65. [[CrossRef](#)]
6. J. Alberto Castañeda, Francisco J. Montoso, Teodoro Luque. 2007. The dimensionality of customer privacy concern on the internet. *Online Information Review* **31**:4, 420-439. [[Abstract](#)] [[Full Text](#)] [[PDF](#)]
7. Chiung-Wen (Julia) Hsu. 2007. Staging on the Internet: Research on Online Photo Album Users in Taiwan with the Spectacle/Performance Paradigm. *CyberPsychology & Behavior* **10**, 596-600. [[CrossRef](#)]
8. Andy Chiou, Jeng-Chung Victor Chen, Craig BissetCross Cultural Perceptions on Privacy in the United States, Vietnam, Indonesia, and Taiwan 727-741. [[CrossRef](#)]
9. Horst Treiblmaier, Sandy ChongTrust and Perceived Risk of Personal Information as Antecedents of Online Information Disclosure 341-361. [[CrossRef](#)]
10. The Role of Information Security and Cryptography in Digital Democracy 158-174. [[CrossRef](#)]
11. Andy Chiou, Jeng-Chung Victor Chen, Craig BissetCross Cultural Perceptions on Privacy in the United States, Vietnam, Indonesia, and Taiwan 727-741. [[CrossRef](#)]
12. Theodosios TsiakisThe Role of Information Security and Cryptography in Digital Democracy: 1564-1580. [[CrossRef](#)]