New Media & Society
http://nms.sagepub.com/

A multinational study on online privacy: global concerns and local responses

Hichang Cho, Milagros Rivera-Sánchez and Sun Sun Lim

New Media Society 2009 11: 395
DOI: 10.1177/1461444808101618

The online version of this article can be found at:
http://nms.sagepub.com/content/11/3/395

Published by:
SAGE
http://www.sagepublications.com

new media & society

Los Angeles, London, New Delhi, Singapore and Washington DC
Vol 11(3): 395–416 [DOI: 10.1177/1461444808101618]

ARTICLE

A multinational study on online privacy: global concerns and local responses

HICHANG CHO

MILAGROS RIVERA-SÁNCHEZ

SUN SUN LIM
National University of Singapore, Singapore

Abstract

This study surveyed 1261 internet users from five cities (Bangalore, Seoul, Singapore, Sydney and New York) to examine multinational internet users' perceptions and behavioural responses concerning online privacy. It identified a set of individual-level (demographics and internet-related experiences) and macro-level factors (nationality and national culture), and tested the extent to which they affected online privacy concerns and privacy protection behaviours. The results showed that individual differences (age, gender and internet experience), nationality and national culture significantly influenced internet users' privacy concerns to the extent that older, female internet users from an individualistic culture were more concerned about online privacy than their counterparts. The study also identified three underlying dimensions of privacy protection behaviour – avoidance, opt-out and proactive protection – and found that they distinctly related to the individual and macro-level factors. Overall, the findings highlight the conditional and multicultural nature of online privacy.

Key words
national culture • online privacy • privacy concern • privacy protection behaviour

INTRODUCTION

Personal information privacy is fast becoming one of the most critical issues in today's information-saturated society (Milberg et al., 1995). Surveys (e.g. Consumer Internet Barometer, 2003) show that while in the 1970s 30 percent of consumers claimed to be concerned about privacy, that figure is now more than 80 percent (Dommeyer and Gross, 2003). Such high levels of concern, it is argued, have negative consequences for the broad-scale adoption of the internet and e-commerce (Infocomm Development Authority, 2004; Sheehan, 1999). For example, many internet users who have never made an online purchase identify privacy concerns as a key reason for their inaction (Infocomm Development Authority, 2004; UCLA Center for Communication Policy, 2004).

Online privacy is not only becoming a significant ethical or managerial issue, it is also viewed increasingly as an 'international human rights' issue (Smith et al., 1996). As more companies and organizations become global, it is obvious that online privacy concerns extend beyond a single national culture (Milberg et al., 1995). However, with a few exceptions, previous online privacy studies have been confined to a national scale and paid little attention to multinational or cross-cultural issues.

The purpose of this study is to explore online privacy using the perspective of cultural relativism (Yeniyurt and Townsend, 2003). A multinational survey was conducted on 1261 internet users from five multinational cities – Bangalore, Seoul, Singapore, Sydney and New York – and the study examined how they perceived and coped with online privacy. It also explored what socio-psychological and cultural factors influenced the way that internet users perceived and responded to online privacy. More specifically, it identified a set of individual-level factors (demographic variables and internet-related experiences) and macro-level factors (nationality and national culture) and tested the extent to which the two-level antecedent factors affected online privacy concerns and self-protection behaviours. Overall, this study is guided by the recognition that investigating and addressing privacy issues requires identifying the root causes of privacy concerns (Wang and Petrison, 1993), as well as taking into account the multidimensional and multicultural nature of online behaviour (Bellman et al., 2004).

LITERATURE REVIEW

Concerns about online privacy and antecedent factors

Privacy is a multifaceted notion, encompassing personal autonomy, democratic participation, identity management and social coordination (Phillips, 2004). Central to this multidimensional construct is the desire to keep personal information out of the hands of others: that is, privacy concerns (Westin, 1967). Research has shown that individual perceptions and values affect privacy concern (Buchanan et al., 2006; Joinson et al., 2006).

A number of studies have tested whether concerns about online privacy are a function of demographic variables. Sheehan (1999) found that female internet users were generally more concerned about their personal privacy than male users. Females tended to be less risk-taking and trusting than males in various social settings, including online shopping (Rodgers and Harris, 2003). Additionally, education level and age have been identified as significant factors influencing online privacy concerns. In general, older people (Bellman et al., 2004) and better educated individuals were more concerned about online privacy since they became more sensitive to, or more aware of, potential privacy problems (Milne and Gordon, 1994; Wang and Petrison, 1993).

Several studies examined the relationship between individuals' experiences with the internet and privacy concerns. Internet experience has been operationalized by length and frequency of use (Bellman et al., 2004; Miyazaki and Fernandez, 2001; UCLA Center for Communication Policy, 2004). Bellman et al. (2004) reported that internet users' concerns about online privacy diminished with internet experience. On the one hand, the suggestion is that online privacy concerns should fall gradually as the average level of internet experience rises (Bellman et al., 2004; Consumer Internet Barometer, 2003). On the other hand, Singh and Hill (2003) found the opposite: experienced and knowledgeable internet users were more concerned about online privacy and less likely to shop online. Singh and Hill reasoned that increased expertise might make consumers more cautious about internet usage, since they were more aware of how their data could be collected and used without permission.

In sum, studies have demonstrated that concerns about online privacy vary across a host of individual factors. More specifically, the literature suggests that gender, age and education levels are significant factors affecting online privacy concerns. Hence, this study predicts that:

> H1: Older, more educated and female internet users will be more concerned about online privacy than younger, less educated and male internet users.

Bellman et al. (2004) predicted that perceived risks about online privacy should be tempered as internet-related experience increases. Similarly, Miyazaki and Fernandez (2001) suggested that concerns about online privacy are likely to be derived from the relative novelty of the internet. As such, prolonged internet usage will lead individuals to discover that online privacy risks are often exaggerated and controllable. Hence, this study predicts that:

> H2: There will be a negative relationship between internet-related experiences and online privacy concern.

Online privacy in a multinational context

In addition to the individual-level factors that govern concerns about online privacy, there are some macro-level variables that must be addressed when examining privacy issues (Bellman et al., 2004; Milberg et al., 2000). Ives and Javenpaa (1991) argued that country-to-country differences must be considered when developing and implementing global information systems and applications. These country-specific variables include legal, historical and cultural environments, which might influence how online privacy is viewed (Singh and Hill, 2003). This study focuses on national culture, since a number of studies have found that cultural values have significant effects on various dimensions of information technology (IT) use and behaviour (e.g. Calhoun et al., 2002). With regard to information privacy, Westin (1967) also suggests that every society values privacy in some form, but the expression of this privacy varies significantly across cultures. The following discussion describes how cultural values may influence online privacy concerns among internet users.

Cultural values and information privacy concern

National culture is defined as the collective mindset distinguishing the members of one nation from another (Hofstede, 1980, 1991). National culture influences a person's actions through cultural values, which valorize particular behaviours while discouraging others (Triandis, 1994). Cultural values tend to endure even when other differences between countries are eroded by changes in economics, politics and other external pressures (Hofstede, 1991).

National culture has been found to affect how an individual responds to a potential risk of being exploited in various social contexts (Tse et al., 1988; Weber and Hsee, 1998). Similarly, researchers have postulated that individuals' concerns with privacy can be influenced by their respective cultural values. These researchers used Hofstede's four indices of national culture: individualism, power distance, uncertainty avoidance and masculinity.

The Individualism Index (IND) refers to an individual's independence from organizations or collectivity. People in individualistic cultures tend to place more value on private life, while collectivistic societies accept more easily groups' and organizations' intrusion into the private life of an individual. Therefore, researchers have proposed that individuals in high IND countries would exhibit higher levels of concern for information privacy (Liu et al., 2004; Milberg et al., 1995, 2000).

The Power Distance Index (PDI) refers to the degree of inequality between a less powerful individual and a more powerful one. Although high PDI cultures tolerate greater levels of power inequality, higher scores are associated with greater mistrust of more powerful groups, such as companies. Hence, individuals in high PDI countries would exhibit higher levels of privacy concerns (Bellman et al., 2004; Milberg et al., 1995, 2000).

The Uncertainty Avoidance Index (UAI) measures the extent to which a society feels threatened by uncertain and ambiguous situations and tries to avoid these situations. Higher UAI is associated with high levels of anxiety, stress and concern for security. Hence, concern for privacy may be positively related to UAI (Bellman et al., 2004; Milberg et al., 1995, 2000).

Finally, the Masculinity Index (MAS) refers to the extent to which a society values 'assertiveness, the acquisition of money and things and not caring for others, the quality of life or people' (Hofstede, 1980: 46). High MAS cultures place greater emphasis on material success, and perhaps the economic benefits of using private information over privacy control (Bellman et al., 2004).

Earlier studies which examined cross-cultural differences in information privacy produced somewhat mixed results. Some found significant relationships between national culture and concern, as predicted (Bellman et al., 2004; Milberg et al., 2000). However, these studies also noted that many dimensions of national culture had an influence on privacy in an opposite direction to what was predicted (e.g. UAI in Bellman et al., 2004; PDI, IND and MAS in Milberg et al., 2000). As far as we are aware, there has been no previous study using a large representative sample of multinational internet users as opposed to non-probabilistic, convenient samples (e.g. students or auditors) or small voluntary samples with a threat of self-selection bias. Further, the focus of some studies has been on personal information privacy rather than online privacy per se. Taken together, the findings of previous studies are not only inconsistent, but also make it difficult to evaluate the accuracy of meanings. Thus, it is not known whether people from different countries have the same expectations for privacy online.

As suggested by Westin, privacy 'is a social, cultural and legal concept, all three of which vary from country to country' (1967: 156). For example, in the USA, privacy is seen as a basic human rights issue, entrenched in the

American Bill of Rights. In contrast, the legal systems in Asian societies have tended to overlook individual interests in favour of the collective. According to Lyon:

> The importance of national goals to life in say, Singapore or Japan, has no equivalents in other parts of the world and can permit much higher levels of intrusive surveillance than would be countenanced in surveillance-conscious regions such as Scandinavia. (2001: 93)

For example, in 2003 Singapore introduced the Computer Misuse (Amendment) Act to allow the government to monitor all computer activity and to take 'pre-emptive action' against hackers before they strike (Boey, 2003). Violation of privacy by Asian governments is not uncommon, and there is little or no recognition of privacy in their constitutions (Tam, 2000).

Using Westin's (1967) 'social balance' arguments, Milberg and colleagues argued that 'variations in privacy social balances, under which privacy's states are traded off against other societal values, are prominent even in societies that are rather homogeneous in many other respects' (1995: 67). It might be expected, then, that individuals in different countries should display varying degrees of concern about online privacy. As noted previously, internet users in different countries reside in heterogeneous social conditions which may cause significant differences in the levels of concern across nationalities (Bellman et al., 2004). Specifically, the above literature suggests that internet users from 'Asian' countries (India, Korea and Singapore) should be less concerned about online privacy than those from 'Western' countries (Australia and the USA), since they are used to cultural norms and legal systems that tend to favour collective over individual interests (Lyon, 2001; Tam, 2000). Hence, this study predicts that:

> H3a: There will be significant differences in the levels of concern about online privacy across the five nationalities.
>
> H3b: Internet users from Asian countries will be less concerned about online privacy than those from western countries.

While H3 tests the overall differences across nationalities, it would be valuable to pinpoint the potential causes of such cross-national differences. As reviewed previously, both theoretical arguments and empirical studies generally suggest that cultural values should have significant effects on the way in which internet users perceive a privacy issue. More specifically, previous studies suggest that individuals in high IND, UAI and PDI countries will exhibit higher levels of concern, because they care about independence from the collective, favour security and clear rules and exhibit higher distrust of organizations. However, individuals in high MAS countries will exhibit lower levels of concern, as they are more willing to provide private

information in exchange for potential economic benefits such as convenience. Hence, this study predicts that:

> H4: Internet users in high IND, UAI and PDI countries (and low MAS countries) will exhibit higher levels of concern about online privacy.

Behavioural responses to online privacy: privacy protection behaviour

Another important aspect of online privacy which has not received full research attention is privacy protection behaviour. While many studies have examined the attitudinal dimension of online privacy, very few have extended their focus to the corresponding behavioural aspect.

Regan (2002) claims that information privacy has been defined largely in terms of the rights of individuals to control information about themselves. In the liberal tradition, for example, privacy is viewed as an individualistic value protecting citizens from intrusion (Phillips, 2004). As such, many solutions for privacy protection, for example, remailers, anonymizers, etc., are geared towards granting individuals an independent means of privacy protection rather than having to rely on third-party protection. However, given that individuals engage in rational and calculated choices, it is predicted that individuals are very unlikely to choose such preventive measures because they are more difficult to use and can slow down their online activities (Phillips, 2004; Regan, 1995, 2002). Moreover, it is argued that those solutions are based overwhelmingly on the traditional understanding of privacy as a personal rather than a social, public and collective value (Mason and Raab, 2002; Phillips, 2004). Thus, some researchers have suggested that privacy should be framed as a common good, and that personal information should be conceptualized as a resource that requires protection for the benefit of society as a whole.

While previous studies have made assumptions about why the individual model of privacy protection is not effective (Phillips, 2004; Regan, 2002), empirical research on how and why individuals reject or accept various protective measures is surprisingly rare. Most studies on privacy protection behaviour were conducted in the context of direct marking (e.g. Dommeyer and Gross, 2003), or examined a very limited set of behavioural responses, such as consumer complaint behaviours (Sheehan and Hoy, 1999), or false disclosure of information (Youn, 2005). As such, previous studies often measured one type of protection behaviour and extrapolated their findings to other types of protection behaviours, in spite of the fact that different preventive measures have been developed for different purposes (Phillips, 2004). This is problematic, given that there are separate dimensions of privacy protection behaviours which can be used selectively by different people (Buchanan et al., 2006). Finally, no studies to date have examined how internet users from different countries or cultures use different strategies to

cope with privacy infringement. As such, it is still unknown how internet users perceive a variety of privacy protection measures; how individuals selectively engage in different types of self-protection strategies; and whether individuals display any different patterns of privacy protection behaviours across various social and cultural groups.

To explore these issues, the current study asks the following research questions. First, it attempts to investigate the dimensionality of privacy protection behaviour. With regard to concerns about online privacy, there have been several studies seeking to discover the underlying dimensions of privacy concern (Malhotra et al., 2004; Milberg et al., 2000, 2002; Smith et al., 1996). With a notable exception (Buchanan et al., 2006), few empirical investigations have sought to find the underlying dimensions of privacy protection behaviour. Exploring the dimensionality of protection behaviour would help researchers to identify the salient attributes of various privacy protection behaviours, and how these behaviours are distinctly related to other social psychological variables. Hence, this study attempts to uncover the following:

> RQ1: What are the underlying dimensions of privacy protection behaviours pertaining to online privacy?

In a more practical sense, it is useful for researchers to uncover how internet users with different social and cultural orientations selectively adopt or reject various types of protection behaviours. Given that there is a dearth of studies examining how internet users from different countries or cultures protect their privacy using different strategies, this study explores the following:

> RQ2: What types of protection behaviours do multinational internet users engage in the most? Are there any significant differences in the way that multinational internet users respond to privacy threats?

Overall, it is believed that such empirical information can provide a more accurate and complete picture on how individuals respond to online privacy. This understanding will help policymakers as well as online organizations to develop more effective ways of protecting privacy at both the individual and collective levels.

METHOD

Sample and procedure

Five cities were selected for the survey. Seoul and Singapore were selected because they have among the highest percentage of internet users in Asia. Bangalore was selected because it is India's IT hub. These three Asian cities were counterbalanced by two western cities, Sydney and New York.

According to Hofstede's national culture indices, Australia and the USA rank highest in the IND (90 and 91 respectively). To ensure consistency of survey implementation, a research company with branches in all five cities was hired to conduct all the surveys. The respondents were selected randomly from the research company's panel database, which comprises 35 million internet users in more than 40 countries and is representative of the general internet user population (AC Nielsen, 2005).

Prior to the final survey, a pilot test was conducted using 101 samples from Bangalore ($N = 34$), Seoul ($N = 46$), Singapore ($N = 11$) and Sydney ($N = 10$) in order to check the reliability and validity of the multiple-item measures developed for this study. Several items were dropped or modified due to low internal consistency and inadequate factor loadings. The final survey was in the form of an online, self-administered questionnaire. In total, a set of 82 items was used, including both novel items and some drawn from the existing published privacy literature, definitions and surveys (see 'Measures' below).

Note that the survey questionnaire was translated into Korean for administration in Seoul. It was translated back into English to ensure that the questionnaire had the same linguistic interpretations for all subjects. The total number of respondents for each city was 300 internet users. However, after eliminating unreliable answers, the final sample size per city was Bangalore: 244, Sydney: 280, Singapore: 277, Seoul: 196 and New York: 264.

Measures

Online privacy concern This was measured by a five-item Likert-scale, based on a unidimensional conceptualization of online privacy concerns. Multidimensional construct models such as Concern for Information Privacy (Smith et al., 1996) or Internet Users' Information Privacy Concerns (Malhotra et al., 2004) were not used, due to the constraints of survey length. However, the given items were comprehensive enough to measure the key dimensions of privacy concerns identified in previous studies, such as general concerns about online privacy, collection and control over online privacy ($\alpha = .759$).

Privacy protection behaviour This was measured by 12 items adapted from previous studies (Dommeyer and Gross, 2003; Stark, 2004). The instrument measured the degree to which internet users display different means of self-protection, such as opting out, use of privacy-enhancing technologies, avoiding the internet for transactions, etc. These items were grouped later into three subcategories based on explorative factor analyses.

National culture To compare cultural values across the cities, Hofstede's (1980, 1991) national culture indices were used: PDI, UAI, MAS and IND.

The index ranges from zero to 100, where 100 represents the strongest degree to which the value dimensions manifested in the culture.

Demographic variables and internet-related experiences The survey measured demographic variables such as gender, age, education and personal income. Internet-related experience was measured by the length and frequency of internet use and experience with internet shopping. Given that the internet is used for purposes such as communicating, gathering information and transacting, online shopping experience was distinguished from general internet experience. A combined scale was not created for internet-related experiences, because some items might have unique relationships with online privacy concerns (Miyazaki and Fernandez, 2001). Finally, another related concept, prior privacy invasion, was measured by using the indicator variable, spam (e.g. 'How often do you receive unsolicited email promotions (spam) that you do not remember signing for?').

Privacy self-efficacy Internet users' self-efficacy belief was measured with regard to privacy protection, and this variable was used to check the construct validity of privacy protection behaviour measurement. Privacy self-efficacy was conceptualized as the extent to which the respondents were confident about their abilities to protect themselves from potential threats arising from privacy intrusion. Previously validated measures (Compeau and Higgins, 1995; Rimal, 2000) were adapted and modified to reflect the specificity of the internet. The internal consistency of six items (e.g. 'I am quite confident in my ability to protect my privacy online') was .716.

RESULTS

Descriptive statistics

Table 1 summarizes the characteristics of internet users from the five cities, their levels of concern and privacy protection behaviours. An ANCOVA assessing group differences by nationality, controlling for demographic variables and internet-related experiences, showed that there were significant differences in online privacy concern ($F = 44.13$, $p < 001$) and privacy protection behaviour ($F = 4.19$, 34.53, 39.56; $p = .002$, 001, 001) across the five nationalities. The comparison between Asian ($M = 5.25$) and western ($M = 5.61$) countries with the same control variables also showed that the difference in online privacy concern was significant ($F = 4.88$, $p = .027$). The results support H3a and H3b.

Antecedent factors affecting privacy concern

H1, H2 and H4 predicted that concerns about online privacy would be a function of demographic variables, internet experiences and national culture, respectively. To test the hypotheses, multiple regression analysis was performed. Prior to hypothesis testing, the key assumptions for regression

• Table 1 Descriptive statistics of measures

	Bangalore	New York	Seoul	Singapore	Sydney	Total	F (p)
Age	27.39	40.86	30.97	28.49	35.33	32.77	78.38
	(10.47)	(10.61)	(10.18)	(7.43)	(11.43)		(.000)
Gender (male/ female)	162/82	126/138	111/85	152/125	155/125	706/555	–
Monthly income★	26,291 (46,914)	5,098 (2,690)	2,432,110 (1,186)	3,123 (1,776)	5,300 (3,065)	–	–
Education★★	60.3%	89%	61.5%	88.8%	81.3%	77.5%	–
Concern	4.57	5.62	5.20	5.91	5.60	5.41	81.331
	(.93)	(.91)	(.86)	(.86)	(.97)	(1.01)	(.000)
Avoidance	4.74	4.10	4.46	4.34	3.98	4.30	13.515
	(.99)	(1.41)	(1.05)	(1.37)	(1.51)	(1.33)	(.000)
Opt-out	4.67	6.03	5.02	5.91	5.79	5.53	65.602
	(1.07)	(1.11)	(1.24)	(1.15)	(1.23)	(1.28)	(.000)
Proactive	4.66	5.02	4.07	5.34	4.70	4.80	42.547
	(.86)	(1.16)	(1.18)	(.97)	(1.29)	(1.17)	(.000)

( ) = *SD*; ★ in local currency; ★★ above high/secondary school.

analysis were checked, such as linearity, normal distribution, constant variance and multicollinearity. No significant violations of those assumptions were found, except for high intercorrelations among the four national culture indices. Hence, the two national culture indices (PDI and MAS) were excluded from the final regression analysis in order to avoid high multicollinearity. IND and UAI were selected because IND is correlated very strongly with PDI (r = -.836) and MAS (r = .922), therefore IND alone can represent the other two; among the four cultural indices, IND is considered to be the key dimension (Triandis, 1994); and the correlation between IND and UAI was relatively low (r = .155).

The final model included the demographics of individuals (age, gender, education and income), internet-related experience (length and frequency of internet use, length and amount of online shopping and spam) and two national culture indices (IND and UAI). Table 2 reports the results of the regression analysis. With regard to H1, age and gender displayed significant associations with online privacy concern (b = .096, p < 001; b = -.072, p = .009). Consistent with the previous literature (e.g. Bellman et al., 2004), older, female internet users were more concerned about online privacy than their younger, male counterparts. Internet users with a higher educational background also tended to be more concerned about online privacy, although the relationship was only marginally significant (b = .050, p = .095). Hence, H1 is supported.

• Table 2 Results of multiple regression analysis predicting levels of concern

Independent variables	*b*	*p*
Cultural factors		
IND	.131	.001
UAI	–.075	.007
Demographic factors		
Age	.096	.001
Gender	.072	.009
Education	.050	.095
Income	–.002	N.S.
Internet–related experience		
Length of internet use	.154	.001
Frequency of internet use	.033	N.S.
Length of internet shopping	–.073	.001
Internet shopping spending	.018	N.S.
Spam	.151	.001

R^2 (adjusted) = .126 (.119).

As for H2, internet-related experiences such as length of internet use (b = .154, $p < 001$) and length of internet shopping (b = -.073, $p < 001$), had significant effects on online privacy concern. Additionally, spam was a significant predictor of privacy concern (b = .151, $p < 001$). It seems that individuals' prior experiences with privacy invasion (e.g. spam) led to higher levels of concern about privacy.

It is interesting to note that while concerns about privacy were associated positively with the length of internet use, it was associated negatively with the length of online shopping. This might be because more experienced internet users are more aware of potential threats, or have had more direct or indirect experiences of privacy intrusion. Despite these concerns, internet users have no choice but to persist in going online, as the internet is a key channel of information or communication. More experienced online shoppers are also likely to have more direct or indirect experiences of privacy intrusion. However, the fact that they persist in shopping online even though the internet is not their only shopping option suggests that they have enhanced through extended usage their personal ability to protect their online privacy. Note that the findings are based on correlational analyses, making it difficult to establish causality. For example, it can be argued that since concern with online privacy prevents many internet users from shopping online (Infocomm Development Authority, 2004), those who shopped online had low privacy concerns to begin with, suggesting that the causal direction can go the other way. Taken together, H2 is supported partially. The findings suggest the

importance of distinguishing online consumers from general internet users and online shopping experience from general internet usage.

With regard to H3, the two cultural indices, IND ($b = .167$, $p < 001$) and UAI ($b = -.120$, $p < 001$) had significant associations with the dependent variable. For IND, the results indicate that individuals from an individualistic culture are more likely to be concerned about online privacy. For UAI, the beta coefficient of UAI was negative, which is opposite to the original hypothesis. Hence, the results provide partial support for H4.

Privacy protection behaviour

A series of explorative factor analysis using a principal component analysis with promax rotation was performed to discover the underlying dimensions of privacy protection behaviour (RQ1). Given that no previous theoretical study examining the dimensionality of privacy protection behaviour was found, explorative factor analysis was used instead of confirmatory factor analysis. Oblique rotation (promax) was appropriate because of the likelihood that the factors would correlate with one another.

Three factors with eigenvalues greater than 1 were retained initially. The scree plot suggested that a three-factor solution was tenable, with factors after the third accounting for smaller proportions of variance. The Kaiser-Meyer-Olkin statistic was 0.795, indicating moderate to moderate-high intercorrelations among items without severe multicollinearity. The study adopted an additional procedure in order to maximize factor purity (i.e. create a set of factor-univocal scales), which suggests that the item's loading on the marked factor should be at least twice the value of the next highest loading (Saucier, 1994).

As shown in Table 3, the results of the final factor analysis indicate the presence of three distinctive factors: 'avoidance' (three items), 'opt-out' (two items) and 'proactive self-protection' (six items). The avoidance factor consists of items such as 'use of non-internet means to communicate, buy, or gather information'. The opt-out factor has to do with actively choosing not to receive email solicitations. The proactive protection factor addresses the more active protection of personal information, using privacy enhancing technologies, erasing cookies, checking trust marks, etc. One item, 'make sure that the financial information is encrypted', was dropped from the final factor analysis because the cross-factor loading was more than 0.40. The final 11 items had factor loadings greater than .60 on the same factor (except for 'privacy policy', of which the factor loading was .587) and cross-loadings fewer than .40 on any other factors, indicating satisfactory convergent and discriminant validities. Internal consistency reliabilities measured by Cronbach's alpha ranged from .66 to .78, sufficient for exploratory analyses. Altogether, the three factors explained 58.97 percent of the variance.

Overall, the results indicate that internet users tend to distinguish distinctive types of privacy privacy protection strategies and that internet users' privacy protection behaviours can be represented by mainly three underlying factors.

To test further the construct validity of the three behavioural factors identified in this study, the ways in which these factors were associated with two theoretically central variables – concern and self-efficacy – were examined. According to protection motivation theory (Rogers, 1975, 1983) and the Extended Parallel Process Model (Witte, 1992), concern and self-efficacy are the most critical variables affecting individuals' risk-coping behaviours. Concern influences individuals' adoption of coping behaviours, as those with high levels of concern are more motivated to think about and act upon a problem to reduce vulnerability to threat. Self-efficacy, defined as the perceived ability to exert personal control in behaviour change (Bandura, 1977), is another central variable affecting individuals' adoption or use of preventive behaviour (Rimal, 2000).

To examine the theoretical relationships between concern and self-efficacy and the three sets of privacy protection variables, hierarchical regression

• Table 3 Results of explorative factor analysis

	Component		
Items	Factor 1 proactive protection	Factor 2 avoidance	Factor 3 opt-out
To avoid violations of my online privacy, I:			
Make sure that the site has at least one trust mark	**.776**	–.145	–.027
Erase my cookies after every online session	**.737**	.057	–.119
Use software programs that block cookies	**.664**	.073	.064
Use software programs that protect my anonymity	**.653**	.164	.027
Make sure that the server (i.e. https) is secure	**.622**	–.192	.292
Check the website or e-commerce vendor's privacy policy	**.587**	.129	–.089
Use non-internet means to communicate with other people	.033	**.841**	–.067
Use non-internet means to gather information and news	.126	**.794**	–.106
Use non-internet means to buy products and services	–.080	**.720**	.296
Opt out of email solicitations	–.109	.121	**.873**
Opt out or prevent third parties from using my personal information for marketing purposes	.079	–.066	**.831**
Variance explained	31.6%	16.7%	10.6%
Inter-factor correlations Factor 1	1.00	.183	.397
Factor 2	.183	1.00	.030

analyses were conducted. In the first step, a set of control variables (demographics, internet experiences and national culture) were included; in the second step, privacy concern and self-efficacy were entered to predict the three dimensions of privacy protection behaviours. The key assumptions for regression were checked and only IND and UAI were included in the model for the same multicollinearity problem noted previously. Table 4 reports the results of three hierarchical regression analyses performed. As shown, some control variables (e.g. demographics) had significant effects on the dependent variables. The addition of two central variables (concern and self-efficacy) significantly improved the model's fit for all three dependent variables. Concern had significant effects on all three dimensions of

• Table 4 Hierarchical regression analyses predicting self-protective behaviors

		Avoidance		Opt-out		Proactive	
Model	Independent variables	*b*	*p*	*b*	*p*	*b*	*p*
1	IND	.047	NS	.219	.001	.348	.000
	UAI	.077	.019	–.211	.001	–.179	.000
	Age	.039	NS	–.059	NS	.033	NS
	Gender	.006	NS	–.009	NS	.002	NS
	Education	.010	NS	.054	.000	–.023	NS
	Income	.017	NS	–.085	.009	–.060	NS
	Length of internet use	–.041	NS	–.019	NS	–.059	NS
	Frequency of internet use	–.051	NS	–.019	.000	.018	NS
	Length of internet shopping	–.214	.001	–.010	.039	–.034	NS
	Internet shopping spending	–.034	NS	–.001	NS	.009	NS
	Spam	–.013	NS	.092	.004	.032	
2	IND	–.007	NS	.166	.000	.239	.001
	UAI	.136	.001	–.165	.000	–.051	NS
	Age	.054	NS	–.059	NS	.075	.012
	Gender	.013	NS	–.010	NS	.021	NS
	Education	.015	NS	.054	NS	–.010	NS
	Income	.024	NS	–.080	.011	–.045	NS
	Length of internet use	–.041	NS	–.021	.012	–.060	NS
	Frequency of internet use	–.049	NS	–.015	NS	.021	NS
	Length of internet shopping	–.197	.001	.038	.002	–.010	NS
	Internet shopping spending	–.036	NS	–.007	NS	.007	NS
	Spam	–.022	NS	.069	NS	.023	NS
	Self-efficacy	.109	.001	.027	NS	.273	.001
	Concern	.160	.001	.234	.000	.272	.001
R^2	Model I	.074	(.064)	.103	(.093)	.130	(.120)
(Adjusted)	Model II	.107	(.096)	.154	(.143)	.262	(.252)
***F* change**			.001		.001		.001

NS = non-significant.

protective behaviour. Similarly, self-efficacy had effects on 'avoidance' and 'proactive protection' but not on 'opt-out'. Note that self-efficacy had more direct influence on 'proactive protection' and relatively less significant or insignificant effects on 'avoidance' and 'opt-out'. It is believed that the level of required effort relative to each individual's level of motivation provides a plausible explanation. Proactive protection strategies require greater effort to find, initiate and use (e.g. use of privacy enhancing technologies). On the contrary, since avoidance or opt-out are relatively straightforward and do not require a high level of computer skills, individuals' beliefs on self-efficacy did not matter significantly.

Overall, the results suggest that concern, self-efficacy and risk behaviour (privacy protection) are closely interlinked, as predicted in protection motivation theory (Rogers, 1975, 1983) and the Extended Parallel Process Model (Witte, 1992). Hence, some initial evidence of construct validity was provided.

Table 1 summarizes the comparison of protection behaviours across the five nationalities (RQ2). It shows that 'opt-out' was the most utilized strategy for privacy protection for internet users in all cities except for Bangalore. 'Avoidance' was the least used strategy in Sydney, Singapore and New York. This suggests that as the internet becomes an essential tool for daily life, people tend to seek out means to protect their online privacy rather than avoid using the internet. However, surprisingly, the internet users in Bangalore and Seoul were more likely to avoid the internet than to use available means to protect their privacy.

DISCUSSION

The present study examined internet users' perceptions and behavioural responses concerning online privacy using a representative sample of multinational internet users. It empirically identified a set of individual and cultural factors affecting online privacy. It also extended the focus of privacy research into the behavioural dimension of online privacy (i.e. privacy protection behaviour) to produce a more complete picture of online privacy. Thus, the findings constitute meaningful contributions to the emerging base of information privacy research, and provide the basis for specific recommendations to those managing personal data in a multinational environment.

First, the present study confirms that online privacy is a significant concern affecting many internet users across countries. According to the survey, more than 70.1 percent of multinational internet users were somewhat or highly concerned about online privacy. Moreover, it was demonstrated that the ways in which individuals perceived and coped with online privacy varied across a host of micro and macro level factors such as age, gender, education, internet experience, nationality and cultural values. Specifically, demographic values

and internet-related experience had significant effects on privacy concerns, largely confirming the findings of previous studies (Bellman et al., 2004; Milne and Gordon, 1994). The study also found that internet users' concerns and behavioural responses varied significantly across nationalities (H3), and that such multinational differences could be explained partially by national culture values (H4). More specifically, internet users from countries with a high IND culture exhibited higher levels of concern about online privacy. As mentioned previously, high individualism is associated with a strong desire for private life and independence from the collective. Consequently, individuals in high individualism countries are more likely to be concerned about potential privacy intrusion. In this regard, the concept of low versus high context communication (Hall, 1977) may help to explain this tendency. Hofstede (1991) concluded that high IND is often linked to low context: that is, direct and detailed communication. Internet users in high IND countries would favour low context communication, and therefore when engaging in online transactions, they would prefer that all transaction-related information be highly explicit and clearly spelled out, perhaps manifesting itself as a higher level of concern about online privacy. In contrast, internet users in low IND, high-context cultures are accustomed to more indirect communication and do not seek explicit details on privacy protection. This suggests that organizations should be conscious of such distinctions when operating in high individualism versus low individualism cultures.

Overall, the findings generally support the 'conditional' nature (McGrath, 1994) and cultural relativism of online behaviours and attitudes (Yeniyurt and Townsend, 2003). This suggests that a more comprehensive and holistic analysis of online privacy is needed, given that how people perceive and respond to online privacy is affected not only by micro-level, individual differences but also by macro-level, national and cultural differences. Rather than assuming that the online population is homogenized due to the forces of globalization, governments and corporations must be cognisant of the prevailing cultural and individual differences that influence internet users' behaviour vis-à-vis online privacy. Indeed, even macro-level national cultural differences will be harder to grasp as globalization and the growth of diasporic cultures give rise to hybrid identities, rendering difficult the assumption that national identities either can, or will, be homogenous and unitary.

Another important finding in this study is that internet users' behavioural responses to online privacy, that is, their privacy protection behaviours, are multidimensional in nature. Today's internet users can adopt various privacy protection measures ranging from passive, effortless strategies to more proactive, cognitively intensive behaviours. The presence of the three unique factors identified in this study suggests that internet users tend to distinguish and exhibit distinctive types of privacy protection behaviours. In other words, different people may be able to protect their privacy in

different ways, implying that individuals' choice of privacy protection behaviour is heterogeneous and conditional rather than homogeneous and universal. Additionally, the three dimensions of protection behaviour were linked distinctly to different sets of antecedent factors, further supporting the multidimensional nature of privacy protection behaviour (see Table 4). The study found that demographic, individual and cultural values influenced the way in which people coped with online privacy. However, the way that these factors influenced protection behaviours varied according to the nature of the behaviour (e.g. 'age' had a significant effect on 'proactive' strategies, but not on others). The findings suggest that, rather than assuming that all approaches to privacy protection are the same, future researchers should be aware of this multidimensional nature of privacy protection behaviour in order to understand fully how different dimensions of privacy protection behaviours are adopted (or rejected) selectively by various social and cultural groups.

Considered broadly, the findings demonstrated empirically the complex and interconnected nature of relationships between individual differences, national cultural values, privacy attitudes and behavioural responses. The study also highlighted the importance of recognizing the multicultural and multidimensional nature of online behaviour in an attempt to theorizing privacy online.

Implications of the study

There are several practical implications of this study. First, although there were marked differences across nationalities, the overall level of privacy concern among multinational internet users was remarkably high. It was found that high levels of concern led to avoidance strategies among internet users (see Table 4), making them resort to alternative means to gather information, shop and communicate. As Buchanan and colleagues (2006) state, online privacy is a complex, multifaceted issue that involves individuals' concerns about how information is gathered, stored, used and shared by numerous actors in a multitude of environments (e.g. medical, educational or commercial). Hence, regulators, government officials, educational institutions, e-commerce vendors and a host of other organizations should take note of the findings of this study and introduce policies that reduce individuals' concerns about potential privacy violations. We also propose that corporate and non-corporate actors should adopt ethical and moral standards, not just policy statements, in confronting online privacy concerns. Embracing such coherent ethical guidelines is essential for building inclusive knowledge societies.

The national and cultural differences observed in this study seem to suggest that online companies and regulatory bodies should embrace a multinational approach to the development of systems utilizing personal data or regulatory

regimes, by crafting country-specific solutions. Additionally, it may be appropriate to pay even more attention to privacy controls in countries where levels of concern are the highest, and where the cultural values appreciate tighter control of personal privacy.

CONCLUSION

Direction for future studies

With the increasing importance of the internet as a cross-border information and transaction tool, online privacy becomes a critical issue for individuals, corporations, regulatory agencies, etc. Analysing how individuals in different countries and cultures view and respond to privacy issues provides a means for researchers to understand further complex online behaviours in the information age. We believe that the present findings provide important observations about multinational internet users and the nature of their concern and behaviour pertaining to online privacy.

A number of issues require further research. First, this study treated information privacy concern as a unidimensional construct. As a result, this study does not explore fully the multidimensional nature of those concerns as with Concern for Information Privacy (Smith et al., 2000) or Internet Users' Information Privacy Concerns (Malhotra et al., 2004). However, Stewart and Segars (2002) suggest that Concern for Information Privacy may be represented more parsimoniously as a higher-order single factor structure. Similarly, Buchanan et al. (2006) suggested that a single-factor solution should be plausible for privacy concern measurement. Nonetheless, future research may employ a multidimensional model of online concern in order to examine how various dimensions of privacy concern are associated distinctively with different types of privacy protection behaviours.

Limitations of the study

It can be argued that the present study failed to account for the effects of another critical factor, that is, the regulatory differences across the five cities, which can have a significant influence on internet users' privacy orientations (Milberg et al., 2000). This study did not measure this variable because an adequate and up-to-date index to examine these differences properly was not available, and developing one was beyond the scope of this work. Nonetheless, based on Milberg et al's (2000) Regulatory Models of Government Involvement in Corporate Privacy Management, the five countries studied fell mostly in the low range of Milberg's regulatory continuum. For example, they mostly follow a 'hands-off' approach or promote corporate self-regulation and have sectarian laws dealing with the most serious types of privacy concerns, such as in the area of banking. Therefore, while for the purposes of this study it was assumed that there

would be no significant differences across the five countries, it is recognized that failing to study the impact that such differences could have on the findings is a limitation that should be noted.

Finally, the present study is limited in that data were gathered using an online survey. Although the study represents a relatively more reliable sampling frame, probability sampling method and sufficient sample size than those used by other studies, the external validity of online samples remains a problem. Since the internet has no central registry of users to create a reliable sampling frame, this limitation might be unavoidable. Hence, the findings of this study should be validated further by research employing various sampling strategies and frames.

Acknowledgements

This study was supported by a grant from National University of Singapore (R-124-000-006-112). The authors thank the editor and the anonymous reviewers for their helpful comments.

References

AC Nielsen (2005) 'Are Online Surveys as Accurate as Offline Surveys?', URL (consulted February 2006): http://www2.acnielsen.com/pubs/2005_q1_ap_surveys.shtml

Bandura, A. (1977) *Social Learning Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bellman, S., E.J. Johnson, S.J. Kobrin and G.L. Lohse (2004) 'International Differences in Information Privacy Concerns: a Global Survey of Consumers', *The Information Society* 20(5): 313–24.

Boey, D. (2003) 'Tough New Laws To Foil Hacking Attacks', *Straits Times* (Singapore), 11 November, p. 1.

Buchanan, T., C.B. Paine, A.N. Joinson and U.-D. Reips (2006) 'Development of Measures of Online Privacy Concern and Protection for Use on the Internet', *Journal of the American Society for Information Science and Technology* 58(2): 57–165.

Calhoun, K.J., J.T.C. Teng and M.J. Cheon (2002) 'Impact of National Culture on Information Technology Usage Behavior: An Exploratory Study of Decision Making in Korea and the USA', *Behavior and Information Technology* 21(4): 293–302.

Compeau, D. and C. Higgins (1995) 'Computer Self-efficacy: Development of a Measure and Initial Test', *Management Information Systems Quarterly* 19(2): 189–211.

Consumer Internet Barometer (2003) 'Consumers Continue Flocking to the Internet: Usage, Satisfaction and Trust Continue to Improve', press release, 3 April, URL (consulted February 2006): http://www.consumerInternetbarometer.us/press.htm

Dommeyer, C.J. and B.L. Gross (2003) 'What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness and Use of Privacy Protection Strategies', *Journal of Interactive Marketing* 17(2): 34–51.

Hall, E.T. (1977) *Beyond Culture*. New York: Anchor-Doubleday.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work Related Values*. Beverly Hills, CA: Sage.

Hofstede, G. (1991) *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill.

Infocomm Development Authority (2004) 'Annual Survey on Infocomm Usage in Households and by Individuals for 2004', URL (consulted February 2006): http://

www.ida.gov.sg/idaweb/factfigure/infopage.jsp?infopagecategory=&infopageid=I3350&versionid = 6
Ives, B. and S.L. Javenpaa (1991) 'Applications of Global Information Technology: Key Issues for Management', *Management Information Systems Quarterly* 15(1): 33–49.
Joinson, A.N., C. Paine, T. Buchanan and U.-D. Reips (2006) 'Watching Me and Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom', *Journal of Information Science* 32(4): 334–43.
Liu, C., J.T. Marchewka and C. Ku (2004) 'American and Taiwanese Perceptions Concerning Privacy, Trust and Behavioral Intentions in Electronic Commerce', *Journal of Global Information Management* 12(1):18–40.
Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
McGrath, J.E. (1984) *Groups Interacting with Technology*. Thousand Oaks, CA: Sage.
Malhotra, N.K., S. Kim and J. Agarwal (2004) 'Internet Users' Information Privacy Concern (IUIPC): The Construct, the Scale and a Causal Model', *Information Systems Research* 15(4): 336–55.
Mason, D. and C.D. Raab (2002) 'Privacy, Surveillance, Trust and Regulation: Individual and Collective Dilemmas of Online Privacy Protection', *Information, Communication and Society* 5(3): 379–81.
Milberg, S.J., S.J. Burke, H.J. Smith and E.A. Kallman (1995) 'Values, Personal Information, Privacy and Regulatory Approaches', *Communications of the ACM* 38(12): 65–74.
Milberg, S.J., H.J. Smith and S.J. Burke (2000) 'Information Privacy: Corporate Management and National Regulation', *Organization Science* 11(1): 35–57.
Milne, G.R. and M.E. Gordon (1994) 'A Segmentation Study of Consumers' Attitudes Toward Direct Mail', *Journal of Direct Marketing* 8(2): 45–52.
Miyazaki, A.D. and A. Fernandez (2001) 'Consumer Perceptions of Privacy and Security Risks for Online Shopping', *Journal of Consumer Affairs* 35(1): 27–44.
Phillips, D.J. (2004) 'Privacy Policy and Pets: The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies', *New Media & Society* 6(6): 691–706.
Regan, P. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill, NC: University of North Carolina Press.
Regan, P. (2002) 'Privacy as a Common Good in the Digital World', *Information, Communication and Society* 5(3): 382–450.
Rimal, R.N. (2000) 'Closing the Knowledge–Behavior Gap in Health Promotion: The Mediating Role of Self-efficacy', *Health Communication* 12(3): 219–237.
Rodgers, S. and M.A. Harris (2003) 'Gender and e-Commerce: An Exploratory Study', *Journal of Advertising Research* 43(3): 322–9.
Rogers, R.W. (1975) 'A Protection Motivation Theory of Fear Appeals and Attitude Change', *Journal of Psychology* 91(1): 93–114.
Rogers, R.W. (1983) 'Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation', in J. Cacioppo and R. Petty (eds) *Social Psychophysiology: a Sourcebook*, pp.153–76. New York: Guilford Press.
Saucier, G. (1994) 'Mini-markers: A Brief Version of Goldberg's Unipolar Big-five Markers', *Journal of Personality Assessment* 63(3): 506–16.
Sheehan, K.B. (1999) 'An Investigation of Gender Difference in On-line Privacy Concerns and Resultant Behaviors', *Journal of Interactive Marketing* 13(4): 24–38.
Sheehan, K.B. and M.G. Hoy (1999) 'Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns', *Journal of Advertising* 3(3): 37–51.

Singh, T. and M.E. Hill (2003) 'Consumer Privacy and the Internet in Europe: A View from Germany', *Journal of Consumer Marketing* 20(7): 634–51.
Smith, H.J., S.J. Milberg and S.J. Burke (1996) 'Information Privacy: Measuring Individuals' Concerns about Organizational Practices', *Management Information Systems Quarterly* 20(2): 167–96.
Stark, D. (2004) 'TNS-TRUSTe Consumer Privacy Index Q4 2004: Consumer Behaviors and Attitudes about Privacy', URL (consulted February 2006): http://www.truste.org/pdf/Q4_2004_Consumer_Privacy_Study.pdf
Stewart, K.A. and A.H. Segars (2002) 'An Empirical Examination of the Concern for Information Privacy Instrument', *Information Systems Research* 13(1): 36–49.
Tam, J.C. (2000) 'Personal Data Privacy in the Asia Pacific: A Real Possibility', Tenth International Conference on Computers, Freedom, and Privacy, Toronto, URL (consulted December 2008): www.cfp2000.org/papers/tam.pdf
Triandis, H.C. (1994) *Culture and Social Behavior*. New York: McGraw-Hill.
Tse, D.K., K.H. Lee, J. Vertinsky and D. Wehrung (1988) 'Does Culture Matter? A Cross-cultural Study of Executives' Choice, Decisiveness and Risk Adjustment in International Marketing', *Journal of Marketing* 52(4): 81–95.
UCLA Center for Communication Policy (2004) 'The UCLA Internet Report: Surveying the Digital Future – Year Four', URL (consulted March 2007): http://www.digitalcenter.org/downloads/DigitalFutureReport-Year4-2004.pdf
Wang, P. and L.A. Petrison (1993) 'Direct Marketing Activities and Personal Privacy: A Consumer Survey', *Journal of Direct Marketing* 7(1): 7–19.
Weber, E.U. and C. Hsee (1998) 'Cross-cultural Differences in Risk Perception, but Cross-cultural Similarities in Attitudes towards Perceived Risk', *Management Science* 44(9): 1205–17.
Westin, A.F. (1967) *Privacy and Freedom*. New York: Athenaeum Publishers.
Witte, K. (1992) 'Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model', *Communication Monographs* 59(4): 329–49.
Yeniyurt, S. and J.D. Townsend (2003) 'Does Culture Explain Acceptance of New Products in a Country? An Empirical Investigation', *International Marketing Review* 20(4): 377–96.
Youn, S. (2005) 'Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–benefit Appraisal Approach', *Journal of Broadcasting and Electronic Media* 49(1): 86–110.

HICHANG CHO is an assistant professor of the Communications and New Media Programme, National University of Singapore. His current research focuses on computer-mediated communication and online privacy.
Address: Communications and New Media Programme, Faculty of Arts and Social Sciences, National University of Singapore, Block AS6, #03–13, 11 Computing Drive, Singapore 117416. [email: cnmch@nus.edu.sg]

MILAGROS RIVERA-SÁNCHEZ is an associate professor and Chair of the Communications and New Media Programme, National University of Singapore. Her current research involves online privacy and its impact on e-commerce in Asia, localization of new media in developing Asia and new media and development. Her work has been published in numerous academic and legal journals in Asia, Europe and the USA. [email: mrivera@nus.edu.sg]

SUN SUN LIM is an assistant professor of the Communications and New Media Programme, National University of Singapore. She has published numerous studies on new media literacy and technology domestication by families and young people in Asia, including China, Singapore and South Korea. [email: sunlim@nus.edu.sg]