Online Privacy Control Via Anonymity And Pseudonym: Cross-Cultural Implications

By: Houn-Gee Chen, **Charlie C. Chen**, Louis Lo And Samuel C. Yang

Abstract

Privacy's exact nature needs to reflect the contemporary view of a society. A growing number of online users demand the protection of their personal privacy via anonymity and pseudonym. The efficacy of these two privacy controls in different online environments is unknown. This study applies social psychology theories to explore the relationship between these personal sentiments—authoritative personality, empathy, fear of negative evaluation, self-esteem, and motives of online privacy rights. We conducted a quasi-experiment by manipulating four online environments (personal e-mail exchange, members-only newsgroup, public newsgroup, and online chat room), and three user identification modes (real name, anonymity and pseudonym). More than 600 subjects from the USA and Taiwan participated in the experimental study. The results of path analysis confirm the effects of some personal sentiments on the motives of online privacy rights. The study concludes with theoretical and practical implications for the roles of privacy in the online society.

Houn-Gee Chen, **Charlie C. Chen**, Louis Lo And Samuel C. Yang (2008) "Online Privacy Control Via Anonymity And Pseudonym: Cross-Cultural Implications" *Behaviour & Information Technology* 27(3), pp.229-242 Version Of Record Available At www.tandfonline.com

1. Introduction

Privacy has continued to be a topic of research interest to the researchers in a number of disciplines, including psychology, sociology, law, and information systems (Dinev and Hart 2004). The emergence and growth of the internet exacerbates the problem of privacy intrusion because it offers ubiquitous accessibility to unknown information seekers. An online safety study shows that 80% of 329 online users in 22 cities across the nation have spyware or adware programs installed without users' awareness (America Online and the National Cyber Security Alliance 2004). The lack of security awareness indicates that privacy rights are becoming exceedingly fragile in the open cyber society.

As such, people are beginning to steer away from privacy-intrusion prone activities such as providing their real names and confidential information to websites. Almost 95% of online users chose not to provide personal information to websites (Hoffman *et al.* 1999). Lack of privacy and trust can have lasting impacts on electronic business, such as decreased purchasing intention (Liu *et al*. 2005), loss of current and prospective customers for business-to-customer (B2C) electronic commerce, and ineffective transactional and information sharing processes for business-to-business (B2B) activities (Preston 2001).

Privacy right is the right to control one's own exposure conditions (Rachels 1975). This kind of privacy right is no longer the default privilege in the cyber society because there is little control over one's personal information. Online users need a stronger faith in humanity now than before (Uslaner 2002). Internet untangles the geographical limitations but increases the risks of having personal information exposed and misused by someone not entitled to it. What is being replaced is the proactive approach of protecting privacy rights by endowing a person with the right to allow or reject the collection, processing, and exploitation of his/her personal information by others. Many functions, such as anonymity, pseudonym, opt-in, opt-out, cookies disabling, firewall, proxy, and anti-spam are available to date, enabling online users to protect personal privacy proactively.

Internet privacy is closely related to cultural and regulatory differences (Bellman *et al*. 2004). The internet is a global phenomenon, and many cyber crimes occur across national boundaries. As a result, countries are beginning to work together to gradually iron out regulatory differences. However, culture has lasting impacts on internet privacy. It is interesting to examine internet privacy from cross-cultural perspectives. Identity representation is a cultural phenomenon that is related to internet privacy. Online users can easily create online identities to express their feelings to other online users with regard to their intended character, goals and origins. People are more likely to engage in the communication process and disclose their personal information in an online environment than in the face-to-face environment (Tidwell and Walther 2002). As such, exercising personal identity is becoming a prevalent practice in the online environment.

Anonymity and pseudonym are two constructive and preventive mechanisms for protecting privacy rights (Coursey 1997, Cranor 1999, Gibbs 1999, McColl Jr. 2000). Anonymity reserves the voluntary rights for a person to act for his/her own benefits by concealing personal identity, and a person's confidentiality is reserved with anonymity. Pseudonym retains both the accountability of real name and the confidentiality of anonymity via identity artifacts, such as user ID and screen name; this privacy control allows an individual to conceal his/her online behavior. Although these two mechanisms give online users some control of what personal information to reveal, they do have limitations. Metcalfe (1994) argues that anonymity puts men in a mask and is the first step in leaping towards a barbaric society. For instance, free e-mail accounts can potentially endanger public interests if someone uses them for malicious purposes, such as the denial-of-service attacks, virus spreading, and unsolicited advertising. The internet differs greatly from the face-to-face environment because social clues, such as pressure to conform to moral standards of a society, are missing. Lack of social clues is more likely to cause misbehaviors, such humiliation, antagonism, and selfishness.

With a higher degree of anonymity control, people are more likely to give honest answers or disclose their confidential information (Turner *et al*. 1998, Tourangeau *et al.* 2003, Tanis and Postmes 2007) in face-to-face and computer-mediated communication settings. In the real name mode, people are least likely to disclose their confidential information when they communicate with others. Pseudonym is a form of social cues that has been adopted by a growing number of people to make them feel comfortable with interacting with others, as well as with releasing and sharing some of their confidential information (Rutter and Stephenson 1979, Culnan and Markus 1987). Variations of the use of pseudonym include the encrypted pseudonym and de-identification of an explicit identifier in the healthcare industry—used to encourage patients to share their sensitive information while protecting their identity (Malin and Sweeney 2004). These three user identification modes—real name, anonymity, and pseudonym—can potential result in changes in human behavior. For instance, anonymity can create more aggressive behaviors than pseudonym and real name (Mü hlenfeld 2005) in the online environment. In addition, online users have more freedom to present themselves in anonymity mode than in pseudonym mode (Walther *et al.* 2001).

The internet puts people in the position of mutual invisibility via anonymity and pseudonym. A person can easily challenge moral dogma of the real world and engage in irresponsible activities in the cyber society. However, have users on the internet stepped towards the barbaric world described by Metcalfe when endowed with the mask of anonymity? To address this question, it is imperative that we investigate the motives of protecting privacy rights using different identification modes and in different online environments.

2. Online privacy issues

Most privacy literatures in the fields of law and philosophy adopt the normative approach of discussing what a human ought to do or how the world ought to be (Davison *et al*. 2003). When applying the normative approach to the changing field of information systems, the quality of privacy research is relatively weak because the ecology of technology, humans, and society is part of the changing process. It is not easy to discuss normatively one or a few moral standards for the correct use of a cutting-edge technology in relation to privacy. Simply, the constant clash between information technology and privacy entails the inapplicability of normative viewpoints. New laws on privacy are continuously being updated and developed to cope with the unpredictable changes and uses of information technology. This concept of the information technology privacy cycle

(Turner and Dasgupta 2003) leads to the belief that privacy rights should not be examined within the definite field of information technology because of technology's unpredictable and disruptive nature.

The descriptive approach appears to be a better alternative to studying privacy in the field of information technology because the objective of this approach is to describe a changing phenomenon, rather than stating right or wrong. Some articles adopt this approach but have scattered comments on occasional privacy intrusion events or the importance of privacy protection in the cyber society (Pottie 2004). There are three descriptive methods to studying privacy: subjective interpretive (interview and case study), pure interpretive (ethnography and action research) and positive interpretive (experimental study) (Lee 1991). This study adopts the positive interpretive method to closely examine and describe the relationship between constructs of interest and privacy rights in different online environments.

People in different cultures have different standards of privacy rights. The cultural dimensions, such as collectivism and power distance (Hofstede 1991) can affect the standards of privacy rights. People in a higher collectivist culture (e.g. Taiwan) have a higher tolerance for sharing their personal information. In Taiwan, it is common to ask a stranger about his/her profession and family background. This cultural effect has probably lessened the confidential effects of free e-mail accounts. For the collective goodwill of an institution or a society, people from the collectivist culture are aware of the prevalence of scrutinous activity in their society. As such, online users do not feel the urgency to protect their privacy rights by demanding a higher morality standard. On the other hand, people from a highly individualistic culture like the USA have little tolerance for institutional scrutiny. Accordingly, people in the USA are less likely than those from the collectivist culture (e.g. China and Singapore) to accept the rationale of collecting their personal information to benefit the society as a whole, and forcing users to fill in their personal confidential information in the USA to authorize the use of a free e-mail account is not likely to be well received. In order to secure privacy rights, Americans demand more privacy rights than people from the collectivist culture. Therefore, it is imperative to examine the impacts of distinctive differences between high and low collectivist cultures with regard to online privacy rights.

2.1 *Motives to exercise online privacy rights*

Privacy rights include family and friendship intimacy, isolation (Pederson 1997), solitude, anonymity and reserve (Westin 1967). The achievement of each privacy right allows people to realize at least one of five benefits: autonomy, confiding, rejuvenation, contemplation and creativity (Pedersen 1997). Westin and Baker (1972) assert that information collection is an inevitable byproduct in the information society. Online users have raised many privacy concerns with regard to the information collection activities by an organization or individual. These concerns include, but are not limited to, unauthorized secondary internal use, unauthorized secondary external use, improper access, data errors, reduced judgment, and the 'mosaic effect' of data combination (Smith *et al.* 1996). Presently, these mal-practises result in numerous privacy intrusion incidents in online environments, which destroy privacy rights and accompanying benefits. Many new online tools are available to help preserve privacy rights in online environments.

Table 1 shows some contrasting examples of the achievement of privacy rights in the real- and cyber-society. For the same privacy right, information systems help online users achieve more benefits. For instance, family members

Table 1. Offline vs. online privacy rights and benefits.

Privacy rights	Offline privacy	Online privacy
Solitude	Office hours (*Autonomy*)	Change my status (busy, taking shower) in the Messenger application (*Autonomy*)
Intimacy with family	Family dinner (*Rejuvenation*)	Online chatting with family members via the chat room with microphone and webcam enabled Creative use of screen names (*Rejuvenation & Confiding*)
Intimacy with friends	Private party (*Confiding*)	Members-only newsgroup (*Rejuvenation, Confiding & Creativity*) Members-only online dating (*Confiding*)
Anonymity	Anonymous polls (*Autonomy*)	Write in the public blogs in the anonymous or acronym mode (*Autonomy, Confiding & Creativity*) Anonymous online survey (*Autonomy, Confiding & Creativity*) IBM's data randomization technique by masking customer data (*Confiding & Creativity*)
Reserve	Mail (Autonomy)	Pseudonym e-mail account Anti-spam software (*Autonomy, Confiding & Creativity*)
Isolation	Take a shower (Rejuvenation & Creativity) Drive alone (Rejuvenation & Creativity)	Enable the feature 'Invisible to Everyone' in the Messenger application (*Rejuvenation & Creativity*)

may feel more comfortable talking to each other in the cyber society than in the physical society. Many social cues (e.g. tones, facial expressions, and hierarchical structure) of the physical world are indiscernible on the internet, and the absence of social clues can lead to the disappearance or alleviation of people's pressures to comply with the established moral standards in the physical society.

As a result, a person can realize not only the benefits of rejuvenation in the physical society, but also those of confiding in the cyber society. A typical example of achieving rejuvenation and confiding benefits is the creative use of screen names. Online environments can potentially mitigate the privacy issue by creating closer relationships between a person and his/her group or community via different media. Media used to help build a closer interpersonal relationship can pressure a person to comply with the moral standards of his/her group or community (Wallace 1999).

The worldwide internet population in 2005 was 1.08 billion and would continue to grow according to Computer Industry Almanac, Central Intelligence Agency's World Factbook and Nielsen/NetRatings (ClickZ Stats 2006). It is important to assess the influence of culture on privacy because the internet is becoming a global phenomenon. A group of people in the same physical proximity, sharing similar values, beliefs and norms gradually develops a collective programming of mind that distinguishes themselves from other groups; that is, culture (Hofstede 1991). Culture influences the formation of an individual's expectations, values, beliefs, attitudes, and behavior (Adler 1991). Privacy standards of an individual are also the result of cultural influence. Hofstede's (1980) theoretical frame- work assesses national culture in terms of four dimensions:
(1) individualism-collectivism, (2) power distance, (3) masculinity-femininity, and (4) uncertainty avoidance. Among these four dimensions, uncertainty avoidance is the dimension that has direct influence on the formation of individual beliefs regarding privacy rights. Individuals from a high uncertainty avoidance culture need more assurance of privacy and security in order to mitigate uncertainty than those from a low uncertainty avoidance culture (Liu *et al.* 2004). This uncertainty reduction can help improve the trust of online users in the use of the technology. Therefore, individuals from different cultures need different levels of online protection control. It is important to assess the effectiveness of identity control mechanisms, such as pseudonym and anonymity, in protecting online privacy.

2.2 *Societal psychological factors of privacy rights*

Many societal psychological factors contribute to the demand of online and offline privacy rights. These factors can be summarized into two native constitutes of the mind: instincts or specific tendencies and non-specific general tendencies. Instincts are an integrated system of cognitive, affective, and conative predispositions. McDougall (1928) defines instinct as 'an inherited or innate psycho-physical disposition' (p. 504). Human beings evolved from low-level species and have inherited four basic instincts: reproduction, gregariousness, acquisition, and construction (McDougall 1928). Emotions are outcomes of the basic instincts. Emotions accompanying these basic instincts include fear, disgust, astonishment, anger, positive self- feeling, negative self-feeling, and tenderness.

Fear is the accompanying emotion of escape. Fear plays a crucial role in the early age of a person when the individual experiences socialization by which society regulates a person's behaviors to meet society's standards. At the early age of moral development, a person has to rely on the anticipation of response, reward or punishment in order to gain self-control. The major effect of anticipation to a response is fear of physical punishment and public opinions.

There are two types of self-regarding sentiments: pride and self-esteem (McDougall 1928). In terms of pride, when a person's behavior meets the moral standard, he/she experiences positive emotions such as joy and self-praise. Pride is composed of the positive emotions. A person will have negative emotions, such as humiliation, misgiving, and a sense of guilty, if that person fails to meet the moral standard. In terms of self-esteem, self-esteem consists of the instincts of self-display and subjection. A person will feel like self-displaying if he/she meets moral standards. Otherwise, a person will feel subjection if he/she fails to meet moral standards.

We argue that the fear of negative evaluation and self-esteem sentiments can also affect the vitality of the online society because online users are interacting with more diversified people in the cyber society than in the real society. For instance, parents have little control over whom their teenager kids talk to in chat rooms. Many online social cues (e.g. icons and pictures) are popular practises in the cyber society that substitute the (missing) physical social clues (e.g. facial and tone expressions). Adopting these social cues shows the importance of sentiments like the fear of negative evaluation and self-esteem in the cyber society.

Authoritative personality and empathy are two antecedent factors of self-esteem and fear of negative evaluation. People respond to authority in many ways. The higher authoritative personality a person has, the easier a person succumbs to authority. A child is afraid of physical punishment and becomes succumbed to the authority. When the child grows older, public opinion replaces physical punishment and becomes a source of authority.

Empathy is the inclination to share emotions or sensation with others. People with a strong empathy sentiment may try to agree with others' emotions if there

is a sensational discrepancy between them and a counterpart. Just as fear is the core element of the authoritative personality, harmony and love are the core elements of empathy, and McDougall (1928) contends that authoritative personality and empathy can prescribe a person's behavioral change in relation to moral standards. These two factors can also help explain why the respect for public opinions has such a strong effect on most people.

Empathy and authoritative personality play crucial roles in moral development, which influences the demand of privacy rights. The emergence of online environments allows people to create different user identification modes such as anonymity and pseudonym. These two user identification modes may change the influence of personal sentiments like authoritative personality and empathy on self-esteem and fear of negative evaluations. As a result, the demand for privacy rights may change accordingly in the cyber environment. This study tries to investigate the causal relationship by manipulating different user identification modes.

2.3 *User identification modes*

This study investigates three primary modes of user identification in the online environment: real name, pseudonym and anonymity. User identification influences a person's urgency to comply with moral standards, and these three modes create different degrees of urgency, which affect the demand for privacy rights.

The real name is the identification of online users in the physical world. It reminds others who are the true owners of the creation (Brin 1998). When a person uses his/her real name, he/she has immediate urgency to comply with moral standards because what a person says and does represents him or her. All personal sentiments are closely linked and contribute to the highest degrees of urgency to comply with moral standards. As such, people will demand privacy rights to avoid revealing themselves in public when they have no intention to do so.

The use of the real name prevails in the physical world because a person needs to account for his/her own behavior according to social norms. Social norms prescribe a reduced acceptance of anonymity in the physical world. On the other hand, anonymity is a popular identification mode in the cyber world because a person does not necessarily need to apply social dogmas of the real world in the cyber society. Anonymity allows a person to realize three categories of benefit: informative utility, eradication of group pressure, and deterrents of law enforcement (Lee 1991), but some weaknesses do accompany these benefits in the use of anonymity (see table 2). With anonymity, personal sentiments are least linked and contribute to the lowest urgency to comply with the moral standard. Since people can choose not to reveal their real identity throughout a cyber social activity, people may not demand privacy rights if they can remain anonymous. Nevertheless, anonymity is more likely than real name to provoke malicious behaviors (e.g. dishonored trade, malicious repudiation, and forgeability). This is so because, in an anonymous situation, an individual could feel less accountable for dishonoured trades and take risks to maximize gains by manipulating pricing and product information. The bid shielding and shilling practice to boost product price via the use of phantom bidders and fake bids in an online auction market is one example of dishonored trade. Although similarly malicious behavior—bid rigging—has long existed in the traditional auctions, the internet eliminates spatial, temporal and geographic constraints and can ease the bid rigging process. Creating multiple user IDs or screen names for the purpose of driving up price is more easily accomplished online. A dishonoured trade can be planned to the exact second for a shielder to drop the highest bid so that he/she using another screen name or his/ her friend can win the auction with a lower offer. Coupled with the growth of online auction activities, dishonoured trades in various forms (e.g. mail fraud and deadbeat bidding) are becoming more prevalent in the online environment. Most online auction sites demand that a trader self reports personal information and creates a user ID before being allowed to trade. Also, the ranking system is another check mechanism adopted by online auction sites to discourage these mal-practices.

Pseudonym is a compromised solution of protecting privacy between these two extremes of user identification modes—real name and anonymity—in cyber space. Here a user can voluntarily choose a pseudonym. E-service providers often recommend an alternative pseudonym if a user's preferred pseudonym is taken. Pseudonyms allow people to access their registered e-services. Some online

Table 2. Strengths and weaknesses of anonymity usage.

	Strengths	Weaknesses
Informative utility	Mitigate the potential prejudice based on the social class	Hard to measure the reliability of information
Pressure of group	Tolerate different opinions in order to protect the freedom of speech	Sacrifice a person's accountability with irresponsible disclosure of information
Enforcement of law	Avoid illegally and unjustified intrusion of a person's privacy by legal entities like government	Difficult to take immediate actions against illegal activities (e.g. copyrights infringement)

users prefer to use e-services anonymously in chat rooms and public newsgroups. People have much freedom to represent themselves with pseudonyms to express their sentiments at a particular moment. The name can be a nickname, or an object, like a pet, car, pillow, hobby, or mood. Since a pseudonym allows a person to create a world of fantasy, the true sentiments, like authoritative personality and empathy, can be deliberately concealed or masked. The use of a pseudonym may underplay the importance of real personal sentiment, which may alter the causal relationship between personal sentiments and a person's demand for privacy rights. It is important to investigate the moderating effect of pseudonym on the causal relationship.

3. Operationalization of research model

When privacy is the domain of research, researchers can improve the research quality by adopting 'reasonably-deep-but-reasonably-broad', instead of 'broad-but-shallow data' (Davison *et al*. 2003, p. 345). This rationale rules out the usefulness of qualitative research methods like case study, ethnography, ground theory, or interview in the area of privacy. The purpose of this study is to investigate the motives underlying different claims of privacy rights in online environments. To examine the contingent causality between motives and privacy rights, our study adopts the quasi-experimental research method to manipulate the moderating factors.

Privacy research is about finding a person's attitude and in general needs to conduct an attitudinal survey. Many extraneous factors can confound the survey results, such as the intrinsic intentions of respondents for each question, unjustified length of statements for Likert scales, and unrepresentativeness of student samples (Davison *et al*. 2003). It is important to assess the phrasing of questions and the collected data about sensitive topics. We, therefore, first tested the validity and reliability of the proposed theoretical framework and survey instruments by conducting a pre-test pilot. This study further manipulated the moderating variables (degree of anonymity and online environment) to understand the variances in the demand for privacy rights between experimental groups and the controllable group. US and Taiwanese subjects participated in the study. The collected data can help us understand the potential influences of culture on the relationship between motives for and claims of privacy rights.

Authoritative personality and empathy are antecedent factors of self-esteem and the fear of negative evaluations, which can influence a person's claim of privacy rights. We propose that an online user would claim different privacy rights in the online environment, varied with different degrees of anonymity. Authoritative personality is a measure of how a person responds to the pressure of authority. This study adopted Adorno *et al*.'s (1950) 16-item questionnaire to measure the reaction. The higher a person scores, the more he/she is submissive to authority. Empathy is a person's inclination to share the feelings or emotions with others. Emotional empathy is a person's vicarious emotional experiences. This study incorporated Mehrabian and Epstein's (1972) Balanced Emotional Empathy Scale (BEES) to measure the empathy variable. The instrument uses 30 items to measure the positive and negative emotional empathy. A subject with a high score is more likely to share his/her feeling or emotions with the others.

Fear is an important factor to orient and civilize people into the society. The fear of negative evaluations (FNE) ranges from physical punishment/reward to positive and negative opinions of the public as a person grows up. This study adopted Watson and Friend's (1969) 30-item instrument, of which 17 items were positively worded items and 13 were negatively worded items. The higher score a person gains in this questionnaire, the higher he/she has FNE.

'Self-esteem is the sense of personal worth and competence that a person associates with his or her self-concept' (Corsini 1984, p. 289). Self-esteem is a multidimensional concept, one key component of a person's self-concept (Corsini 1984). Self-esteem is the source of an individual's feelings about his/her success or failure (Glasser 1965). In other words, self-esteem is a subjective self-display or emotional expression. This study measured the self-esteem construct via two questionnaires. Coppersmith's (1967) 25- item instrument measures a person's positive self-esteem. The higher the score a person gains on this questionnaire, the higher the self-esteem. Rosenberg's (1965) 10-item instrument measures a person's negative self-esteem. The higher a person scores in this instrument, the lower a person's self-esteem.

A person can enjoy many benefits when he/she can declare his/her privacy rights in the event of intrusion. Pederson's Privacy Function Rating Scale (PFRS) measures the benefits of privacy rights claimed by the subject. The higher the subject scores on this questionnaire, the higher a person is inclined to pursue certain benefits of privacy rights. We will also examine the previously mentioned privacy rights in the later section 'Motives of privacy rights' to obtain the micro perspective of the instrument.

The closer interpersonal relationship a medium can help people build, the higher pressures they have to comply with the moral standards of his/her group. We manipulated four online environments based on their ability to create a close relationship between users and their community: e-mail (the highest), members-only newsgroup (the second highest), public newsgroup (the third highest), and chat room (the lowest) (Wallace 1999). This study controls these online environments to investigate their potential moderating effects on the relationship between motives and benefits of privacy rights.

We operationalized three modes of online users' identification based on the structure of e-mail accounts. Subjects provided their e-mail accounts during their participation in this study. Real name identifications are e-mail accounts that end with the domain of an official organization (e.g. school and company). Pseudonym identifications are free e-mail accounts that end with the domain of an internet service provider. Anonymity identifications are subjects choosing not to give any e-mail addresses.

We recruited 625 subjects (333 from Taiwan, and 292 from USA) to participate in the study. Table 3 shows these subjects' gender ratio and age distribution. More female subjects from both countries participated in the study. Subjects were predominately between 21 and 30 years old.

We limited our subject recruitment from three sources: an advertising banner, job news on the bulletin boards on campus, and e-mail invitations. The control mitigates the potential influence of differences in the IT environment of both countries. The detailed information about each source is shown below:

Sources of Taiwanese subjects include:

- Response to the advertising banners of 'People Wanted' posted on the GAIS search engine between March 25 and April 25.
- Response to the Job News, entitled as 'Cash for Questionnaire Filling,' on the bulletin boards of universities in Taiwan.
- Response to an e-mail invitation to students to participate in a survey.

Sources of US subjects include:

- Response to the advertising banners of 'People Wanted' posted on the website of an internet research centre of an US university.
- Response to the 'People Wanted' news announced on campus websites.
- Response to an e-mail invitation for members of information systems associations to participate in the survey.

Table 3. Sample characteristics.

		Taiwan		USA	
Features of background	Categories	No. of samples	Percentage	No. of samples	Percentage
Gender	Male	132	39.6%	137	46.9%
	Female	201	60.4%	155	53.1%
Age	Under 20	83	24.9%	51	17.5%
	21–30	234	70.3%	182	62.3%
	31–40	11	3.3%	47	16.1%
	41–50	3	0.9%	10	3.42%
	Over 50	2	0.6%	2	0.68%

4. Hypotheses

Six hypotheses were proposed and tested to assess the relationship between personal sentiments and privacy rights based on our literature review. Online environments and identification modes are moderating factors influencing the relationship.

A person who was more submissive to authority would have a higher fear when facing the negative evaluation. A person would be more likely to comply with the moral standards without hesitation when the fear of negative evaluation is high.

H1: Subjects with a higher authoritative personality are more likely to have an increased fear of negative evaluations (FNE).

A person who has a higher authoritative personality would have a higher self-esteem because he/she is more concerned with the expectation and evaluation of a person's behaviors by others in the online environment. On the other hand, a person, who is less submissive to authority, would more likely behave at his/her own wills and overlook the moral standards of the society. Moral standards have less influence on subjects who have a lower authoritative personality.

H2: Subjects with a higher authoritative personality are more likely to have a higher self-esteem.

When subjects have an inclination to share their feelings or emotions with others, they have a higher empathy. Empathetic subjects have a higher motive to seek agreement with others in the same group. They are more likely to accept rather than challenge pressures or critiques from their group. These subjects would do their best to accommodate their behaviors in order to alleviate their fear of negative evaluation. Therefore, subjects with a higher empathy are more likely to have an increased fear of negative evaluations by their group members.

H3: Subjects with higher empathy are more likely to have an increased fear of negative evaluations (FNE).

In the compliance with the moral standards, empathetic subjects would increase their satisfaction levels because the sensation and sympathy with other members reinforce the reciprocity of the relationship between them and their group. As such, subjects with higher empathy are more likely to have higher self-esteem.

H4: Subjects with higher empathy are more likely to have higher self-esteem.

A person with increased fear of negative evaluations is more likely to exercise privacy rights—intimacy, isolation, solitude, anonymity and reserve—to avoid the threats of negative evaluation from the group. The exercise of privacy rights could be supported by privacy-enhancing technology, legal remedy or a combination of both. The exercise of privacy rights via privacy-enhancing technology (the focus of this study) can greatly reduce the fear of a subject with a high FNE. On the other hand, subjects with a lower FNE are less interested in exercising their privacy rights.

H5: A person with an increased fear of negative evaluations (FNE) is more likely to exercise his/her privacy rights.

A person with higher self-esteem is more likely to alleviate the pressure of privacy violations by exercising privacy rights. Those with lower self-esteem seldom exercise their privacy rights because they were not obedient to the standards of social morality in exchange for the improvement of their reputations and self-esteem.

H6: A person with higher self-esteem is more likely to exercise his/her privacy rights.

5. Result and discussions

Replicating the same experimental setting in two different cultures can help improve the generalizability of this study. Taiwanese subjects read Chinese while US subjects read English. Translating the original English instruments into Chinese requires extra efforts in measuring the reliability of the original and translated instruments. In addition to Cronbach's alpha testing, we conducted composite reliability and variance of the extracted measures. Composite reliability is a measurement of internal consistency of items used to represent a latent variable. The higher the composite reliability is, the better internal consistency of items for a latent variable. Variance extracted measures the explanatory power of latent variables for the entire variance of total items. The higher the variance extracted value is, the higher explanatory power the items have for latent variables. Structural equation modeling (SEM) is the data analysis method used to conduct confirmatory factor analysis of theoretical constructs to verify the construct validity (see table 4). We also calculated the *t*-score of factors loading on each item to verify their convergence validity. We examined the discriminate validity to verify the correlation coefficient of different factors for each construct. If correlation coefficients were not equal to a person, we could deduce that these factors had discriminate validity. We also provided goodness indexes to represent the extent of matching between model and data.

Three reliability tests showed that items used to represent factor 1 (conventionalism) of the authoritative personality variable are below the acceptable level 0.35. Alpha level was 0.29 in Taiwan and 0.3 in the USA. These items were dropped from the original and translated instrument. Other items adequately represented their factor and variable with the alpha value higher than the acceptable level. They were included in the original questionnaire.

5.1 *Path analysis*

This study adopts path analysis to examine the cause-and-effect relationship between independent and dependent variables. Path analysis requires that a theoretical model includes only relevant causal variables or excludes extraneous variables. The existence of these variables can

Table 4. Validity test of survey instruments.

Variables	Items/Factor	Cronbach's α values	Composite reliability	Extracted variances
Authoritative Personality				
Factor 1	2	0.2948	0.30	0.18
Factor 2	6	0.5309	0.55	0.20
Factor 3	8	0.6194	0.63	0.19
Empathy	9	0.8042	0.80	0.31
FNE	16	0.8955	0.91	0.27
Coppersmith's Self-esteem	10	0.7814	0.75	0.24
Rosenberg's Self-esteem	9	0.8060	0.84	0.37
Benefits of Privacy Rights				
PA	2	0.6932	0.78	0.64
CT	2	0.6506	0.59	0.44
RJ	2	0.5017	0.36	0.22
CF	2	0.5210	0.63	0.47
CR	2	0.7371	0.75	0.62

PA, personal autonomy; CT, contemplation; RJ, rejuvenation; CF, confiding; CR, creativity.

Substantially affect the path coefficients, which would confound the assessment of the relative importance of direct and indirect causal paths to the dependent variables. This study incorporates three relevant independent variables (authoritative personality, FNE and empathy), and extraneous variables (identifications and online environments). Path analysis is a suitable tool to analyze the data against the theoretical model. This study used the Structural Equation Modeling (SEM) package to run the path analysis in lieu of a stand-alone path analysis program because there were multiple observed indicators for each latent variable.

SEM calculated path coefficients (beta) for 10 paths in the theoretical framework (see figure 1). Sample size in anonymous mode was below the reasonable sample size (n ¼ 200) of a SEM test. Therefore, we excluded this extraneous variable from our data analysis.

The path analysis results show that path coefficients are significant for path 3 (the effect of empathy on Rosenberg's negative self-esteem) and path 4 (the effect of FNE on Coppersmith's positive self-esteem) (see table 5). This finding is consistent in four online environments (e-mail, public newsgroup, members-only newsgroup, and chat room) and two cultures (Taiwan and USA). The consistency of the results indicates that the extraneous variables (online environment and culture) do not have an effect on the causal relationship between empathy and self-esteem and between FNE and self-esteem in the path model controlling for other prior variables. This study also does not support other causal relationships.

Coefficients of paths 1 and 2 are not significant. This indicates that the missing social clues in online environments may mitigate the influence of authoritative personality on positive and negative self-esteem. The authoritative personality is a determinant for the formation of positive and negative self-esteem in the physical society. However, without pressure to comply with the morality standard of the physical society, online users with high or low authoritative personality have indifferent response to both positive and negative self-esteem. In other words, other people's expectation and evaluation have little enforcing power to discipline a person's behavior in the online environment. As such, online users are more likely to overlook the moral standards in the online environment.

5.2 *Real name mode*

Coefficients of paths 3 and 4 are significant at the significance level ($P \leq 0.01$) in the real name mode. Testing results show that empathy and FNE have negative and positive effects on the endogenous variable self-esteem, respectively. The first finding indicates that subjects with higher empathy are more likely to have a higher negative self-esteem in the online environment. Empathetic subjects can increase their esteem or satisfaction levels if other members express their sensations and sympathies instead of praises and rewards. The negative self-esteem can reinforce the reciprocity of the relationship between empathetic subjects and their group members.

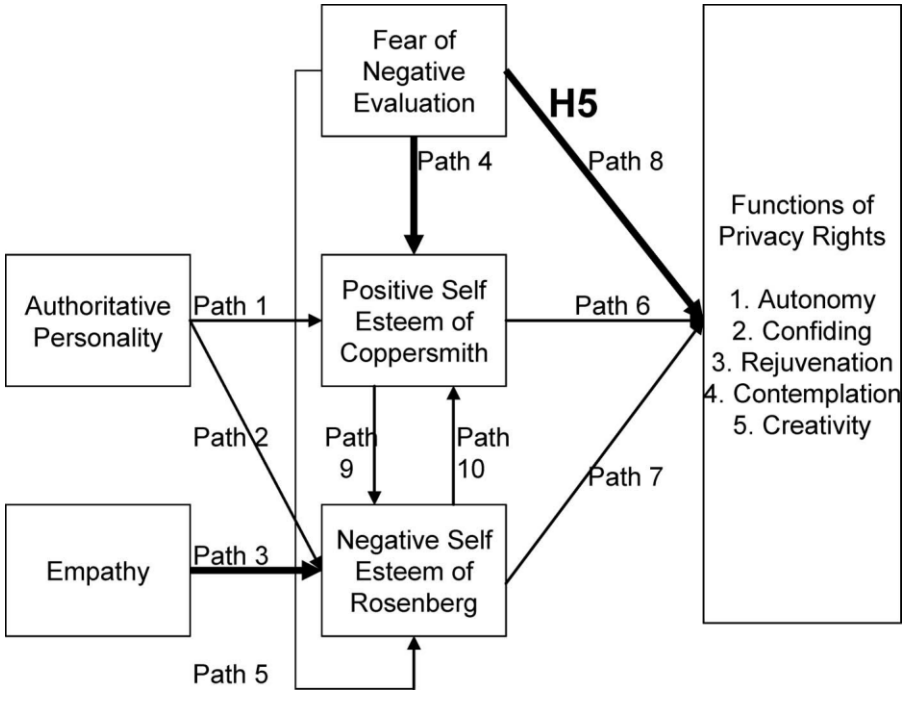

Figure 1. Personal sentiments and online privacy rights model.

Table 5. Summary of path analysis (Taiwan and USA).

Mode	Path 1	Path 2	Path 3	Path 4	Path 5	Path 6	Path 7	Path 8	Path 9	Path 10
RN – Email										
TW	0.18	70.07	0.28**	0.43**	70.04	70.08	0.93	70.36	0.68	0.36
US	0.20	0.01	0.31**	0.45**	70.03	70.02	0.50	70.21	0.50	0.41
RN—Public Newsgroup										
TW	0.07	0.03	0.28**	0.35**	70.15	0.29	0.29	70.23	0.51	0.46
US	0.10	0.09	0.30**	0.36**	70.13	70.10	0.20	70.19	0.45	0.49
RN—Private Newsgroup										
TW	0.08	0.02	0.28**	0.36**	70.14	70.38	0.41	70.14	0.53	0.45
US	0.07	0.05	0.32**	0.35**	70.12	70.35	0.39	70.12	0.40	0.37
RN—Chat Room										
TW	0.10	0.01	0.28**	0.38*	70.11	70.48	0.38	70.23	0.58	0.40
US	0.09	0.05	0.30**	0.37**	70.10	70.43	0.37	70.20	0.40	0.35
PS—E-mail										
TW	70.17	0.14	0.21**	0.30**	70.37	0.03	0.13	0.16	0.18	0.65
US	70.10	0.12	0.24**	0.31**	0.12	0.02	0.12	0.23**	0.10	.050
PS—Public Newsgroup										
TW	70.17	0.13	0.22**	0.28**	0.44	0.17	70.04	0.23**	0.08	0.69
US	70.11	0.13	0.23**	0.29**	0.40	0.15	70.03	0.25**	0.11	0.54
PS—Private Newsgroup										
TW	70.17	0.14	0.21**	0.30**	0.39	0.15	0.05	0.21**	0.15	0.66
US	70.12	0.13	0.23**	0.31**	0.36	0.13	0.04	0.24**	0.12	0.60
PS—Chat Room										
TW	70.17	0.13	0.21**	0.29**	0.41	0.17	0.05	0.23**	0.12	0.67
US	70.11	0.12	0.22**	0.29**	0.40	0.15	0.04	0.23**	0.10	0.59

(**$P \leq 0.01$).

The significance of path 4 coefficient indicates that subjects with a higher fear of negative evaluation (FNE) are more likely to have a higher positive self-esteem in the online environment. As in the physical society, online users adjust their behaviors to match those of online community in order to alleviate their FNE from other group members. Subjects with a higher FNE often expect critique from other group members and are more likely to disguise their behavior. The online behavior helps create positive self-esteem.

However, the relationship between motives of privacy rights and positive or negative self-esteem is not significant. A higher self-esteem in either form has no effects on the urgent demand for the exercise of privacy rights. An online user does not deliberately disclose personal information to increase his/her self-esteem, thereby achieving the benefits of privacy rights. Neither does an online user behave against his/her own will, in order to meet the morality standard of the online society.

5.3 *Pseudonym mode*

Coefficients of paths 3 and 4 are also significant for subjects in the pseudonym mode. One major difference between real name and pseudonym modes is that Hypothesis H5 is supported in the pseudonym mode but not in the real name mode. A higher FNE from other online users has effects on the increased needs of an online user to exercise privacy rights in the pseudonym mode. Online users choose a pseudonym based on their identification that may not represent them in the real world. For instance, a user who is unhappy in the real life may project herself as a happy person by naming herself as 'A Merry Queen' and using that name as her pseudonym in the cyber world. To avoid having the FNE that a person experiences in the physical society, he/she in the cyber world may choose to create another image in pseudonym that is not used in the physical society. This disguised strategy emphasizes the importance of achieving the benefits of privacy rights in online environments. In the comparison between real time and pseudonym modes, the findings indicate that the effect of identification mode on the compliance of moral standards is stronger than that of online environments or communication media.

There is one exception to Hypothesis H5. The result shows that the relationship between FNE and benefits of privacy rights is not significant in the e-mail environment in Taiwan. This finding is the same as in the real name mode. The ignorable effect of FNE on privacy rights in Taiwan has cultural implications. First, online users from both countries have a higher demand for the protection of their privacy rights in public- and private-newsgroups, as well as in online chat room environments, than for the protection of privacy rights in the e-mail environment. The odds of meeting strangers are much higher in the first three environments, which pose a higher challenge of tracking the user identification of

participants and a higher risk of having other online users scrutinize a person's activities without his/her knowledge. As a result, online users feel the pressure and speculate on the negative evaluation from other users. In order to reduce anxiety, a person begins to demand more stringent privacy by exercising his/her privacy rights in order to refrain from FNE. Due to the influence of FNE on the benefits of privacy rights, their causality is significant. Second, the result shows that subjects in Taiwan who engaged in the e-mail exchange activities do not demand more stringent privacy rights because of their FNE. In contrast, US subjects are just as concerned with privacy rights in the e-mail environment as in the other three online environments.

5.4 *Motives of privacy rights*

We further examined the benefits of privacy rights that affect the real name and pseudonym modes. The data show that in the real name and pseudonym modes, creativity and contemplation have significant coefficients in relation to the construct of benefits of privacy rights. However, the other three factors—personal autonomy, rejuvenation and confiding—do not have significant coefficients. These findings show that empathy and FNE are exogenous variables to self-esteem, which can affect creativity and contemplation. However, the other three benefits—autonomy, rejuvenation, and confiding—are not salient in the online environments as they are in the physical society. This evidence indicates that creativity and contemplation are two important benefits that attract online users in engaging in numerous online group activities to boost their self-esteem. On the other hand, a person may choose to face reality, isolate himself, or meet friends face-to-face if his objectives are to achieve autonomy, confiding and rejuvenation; online group activities are a less preferable solution than face-to- face group activities to realize these three privacy benefits.

6. Implications

Our statistical analysis results indicate that online environment and user identification are important extraneous variables that can affect the motives of privacy rights. These two variables need to work together in order to have the effect. One variable alone is not sufficient. In the real name mode, changes in four online environments have no effect on the motives of privacy rights. In any one particular online environment, changing from real name to pseudonym mode also does not have an effect on the motives of privacy rights. However, when user identification and online environment change simultaneously, FNE has a significant effect on the motives of privacy rights. These preliminary findings show that the interaction between online environments and user identification can significantly influence a person's demand for privacy rights.

The findings present some managerial implications. First, a good design of an online community needs to incorporate user identifications. The joint design approach will motivate online users to engage in numerous private activities. However, a person's FNE from other participants may increase. As a result, a person has an urgent demand for privacy rights when adopting user identifications and online communities at the same time. Second, because an entity or a person needs to have legal authorization before starting the tracking process, the online environment is perceived to be a more private place than the face-to-face environment (because of the difficulty in tracking a person's activities). In an online environment, this perception remains but does not transform into a lower demand for privacy rights. Instead, online users have a higher demand for the protection of their privacy rights. One interpretation of this phenomenon is that the indirect use of personal information can be more easily accomplished on the internet than in the physical world, and on the internet it is more likely that people will use personal information of online users without their knowledge. This perception has raised the concerns of users about the control of their personal information. An operational manager of an online community needs to be aware of this perception and of the demand for privacy rights in the online environment. Privacy statements and privacy web surveys are two approaches that can be used to communicate with and educate online users about the information practices of the website. However, each approach alone cannot effectively reduce the FNE of online users. Privacy statements alone do not guarantee that the website follows its own privacy policy, observes fair information practices, and allows online users to take corrective actions if privacy intrusion occurs (Milne and Culnan 2002). Privacy web survey alone has limitations in providing enough insights about a site's corporate policy (Hastak *et al.* 2001). Therefore, an operational manager may want to adopt both approaches to better understand customers and to aggressively eliminate their FNE. A third approach is to understand the authoritative personality and empathy level of online users in a more proactive way. An operational manager also needs to formulate strategies to manage users' personal information by designing an effective mix of online environments and identifications.

Governmental regulations are another alternative to gain the trust of online users. However, a dilemma exists between regulatory enforcement and the protection of personal information because they are different in nature. Some users fear the abuse of their personal information by governmental authorities. Stegeman's (2004) survey shows that 88% of customers believe that the government is the most likely organization that abuses a consumer's privacy rights with cutting-edge technology. Many network security tools, such as encryption, digital signature, and acronym, emerged to help deter the abuse of personal information. However, these

network tools are still operated by human beings. Although the government can regulate the use of these security tools, it cannot regulate the operator's intention to abuse personal information. A hacker who practices social engineering techniques to steal personal information from the authority is an example that illustrates the weakness of current security tools. The extent of governmental involvement with the management of privacy rights for enterprises varies in different countries (Smith *et al.* 1995). The principles of 'fair information practises', initiated by the Organisation for Economic Co-operation and Development (OECD) in 1980, are basic guidelines for many national privacy laws that regulate online activities. The privacy impact assessment (PIA) is an evaluation that proactively assesses the potential impact of national privacy policies on an individual's privacy (Stewart 1996). Countries that are progressive in privacy protection of their citizens have adopted PIA in order to mitigate potential adverse effects of privacy control. These countries include Australia, New Zealand, Canada, the USA, and Hong Kong. The E-Government Act of 2002 explicitly states the importance of conducting PIA when using technology to collect information. 'Federal government agencies would be required to: make information more accessible and useable; provide better privacy notice on the web; and create 'privacy impact assessments' for new information collections' (E-Government Act 2002). Despite some national efforts to protect online privacy, they represent a small percentage of the international community and are primarily located in the developed countries (Banisar 2004). It is clear to us that governmental involvement on a worldwide basis is relatively weak.

Reliance on government involvement is necessary but not sufficient for the protection of an individual's privacy rights. Rather, an operator of a website needs to have a privacy ecology mindset; that is, online users, website operators and authoritative institutions are three key components of privacy ecology. The responsibility of a website operator is to constantly keep a balance of the demands of the three stakeholders.

Cultural differences may also cause changes in the use of online environments. Subjects from different cultures may exhibit somewhat different degrees of motives for privacy rights. For example, an online user needs to provide different types of personal information in order to acquire free e-mail accounts both in Taiwan and in the USA. As a result, the causal relationship between FNE and motives of privacy rights is different.

7. Limitations

This study lacks literature that bridges the gap between legal and psychological views on personal privacy. Future research may want to incorporate joint perspectives when exploring issues on personal online privacy. The exclusion of samples in anonymous mode from the data analysis is another limitation that needs to be overcome in future research. Future studies can increase sample size in order to make a comparison among three identification modes. The treatment can shed light on the effect of different degrees of anonymity on the motives of privacy rights.

The sample in this study had an unequal gender distribution. All subjects are students. Our findings may be more generalizable to the female and non-student population if future research can control subjects' backgrounds. Scholars interested in replicating the study can collect data from commercial websites, such as Geocities and political blogs. Data collected from a business-oriented website can complement the results of this study with respect to external validity.

The theoretical model of this study can potentially incorporate other relevant independent and exogenous variables to improve its explanatory power. Independent variables for the authoritative personality may include the closeness of the authority, the prestige of the setting, and presence of rebellious peers. For instance, a professional online com- munity may have a higher percentage of rebellious peers who frequently challenge a person's ideas. As such, a person may have a higher authoritative personality in this setting, which will affect his/her self-esteem and motives of personal privacy. Also, will the ability to adopt more than one pseudonym affect the motives of privacy rights.

Mason *et al.* (1995) assert that privacy, accuracy, property and accessibility (PAPA) are four key ethical factors to consider when designing information systems to enhance the dignity of mankind. An interesting research question to be asked by future studies is how will a person's freedom to choose among real name, anonymity and pseudonym affect these four ethics factors? Are people in anonymity mode more likely to ignore these four ethics issues than people in real name mode? What is the relationship between personal sentiments and these four ethics factors?

Data sensitivity has different levels of intensity for different groups of users (Culnan 1993). Online users may feel different degrees of urgency to protect their personal data, and the motives for privacy protection may vary with different groups of users (Sheehan and Hoy 2000). For instance, medical data is much more sensitive to a patient than hobby data. Within medical data, family medical history is more sensitive than a single event of illness. As such, online users in the hobby community may be more receptive to online cookie functions than those in the cancer support-group community. Researchers may also want to rank the importance of privacy issues based on data sensitivity and intensity for different online communities. Lessons learned from these future studies will provide valuable guidelines that websites may use to fine-tune their personalization and customization functions to alleviate privacy concerns of users and drive web traffic to their sites.

8. Conclusions

We asked the question in the beginning of the study, i.e. would the pseudonym mechanism lead online users into the creation of Bob Metcalfe's barbarian world, which was ransacked with innumerous personal attack and irresponsible statements? According to our study, online users in pseudonym mode intend to seek the protection of privacy rights due to the increased FNE. However, in the real name mode (a counterpart of the real world) online users' demand for the protection of privacy rights is relatively weak. Meanwhile, FNE or self-esteem has no effect on the motives of privacy rights. This is partly because in the real name environment, a person's rationale, instead of the prediction or suspicion of potential reward or punishment associated with online activities, regulates a person's behavior. In the online environment, the suspicion of potential reward or punishment regulates his/her behaviors. As a result, a person's rationale has a less weighted influence on the demand for privacy rights.

A person's moral development cannot leap forward, but it can fall back under some conditions according to Kohlberg and Turiel (1971). This study demonstrates that in terms of a person's morality standard, using the pseudonym represents a fallback from the rationale-based decision. As such, the prediction and suspicion of negative evaluations from other online members replace the rationale. This results in the increased demand for more stringent protection of privacy rights.

Do our findings indicate that online users need to waive their privacy rights in order to boost their morality? As to this controversy, we cannot jump to a conclusion through a single study. The argument for and against the exercise of privacy rights in the online environment manifests the currency and importance of this issue. Online users are riding with or against the flow of more regulations to protect personal privacy in both real and cyber worlds. People expect that the potential of the cyber world can provide an outlet for their minds, or even create a cyber utopia. Although the utopia never exists, the cyber world indeed offers a place for online users to seek a balance between personal interests and the development of new societal order. Online environments provide many new mechanisms to secure personal privacy, and users online can engage one another in order to carry out more creative activities and thoughtful contemplation without the interference of public enforcement or social norms.

References

Adler, N.J., 1991, *International Dimensions of Organizational Behavior*, 2nd edition (Boston, MA: PWS-Kent).

Adorno, T., Frankel-Brunswick, E., Levinson, D.J. and Sanford, R.N., 1950, *The Authoritarian Personality* (New York: Harper and Row).

America Online and the National Cyber Security Alliance, 2004, AOL/NCSA Online Safety Study.

Banisar, D., 2006, Freedom of information around the world 2006: A global survey of access to government information laws, Privacy International, Retrieved October 31, 2006 at http://www.privacyinternational.org/foi/foisurvey2006.pdf

Bellman, S., Johnson, E., Kobrin, S. and Lohse, G., 2004, International differences in information privacy concerns: a global survey of consumers. *The Information Society*, 20, pp. 313 – 324.

Brin, D., 1998, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (Boston, MA: Addison-Wesley Longman, Inc.).

ClickZ Stats, 2006, Global online populations. Retrieved October 30, 2006, from http://www.clickz.com/showPage.html?page¼stats/web_worldwide

Coppersmith, S., 1967, *The Antecedents of Self-Esteem* (San Francisco, CA: W.H. Freeman & Company).

Corsini, R.L., 1984, *Self-esteem.* In *The Encyclopedia of Psychology.* Vol. 1, (Guilford, CT: DPG Reference) pp. 289–290.

Coursey, D., 1997, Where everybody knows your name. *ComputerWorld*, 31, pp. 6 – 8.

Cranor, L.F., 1999, Internet privacy. *Communications of the ACM*, 42, pp. 28 – 31.

Culnan, M., 1993, How did they get my name?: an exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17, pp. 341 – 365.

Culnan, M.J. and Markus, M.L. (Ed.), 1987, *Information Technologies* (Newbury Park, CA: Sage).

Davison, R.M., Smith, H.J., Clarke, R., Langford, D. and Kuo, B.F.Y., 2003, Information privacy in a globally networked society: implications for IS research. *Communications of the AIS*, 12, pp. 341–365.

Dinev, T. and Hart, P., 2004, Internet privacy concerns and their Antecedents—measurement validity and a regression model. *Behaviour and Information Technology*, 23, pp. 413 – 422.

E-Government Act of 2002., 2002, 107th Congress of United States. Retrieved October 30, 2006 from http://www.whitehouse.gov/omb/egov/g-4-act.html

Gibbs, M., 1999, Responsibility anonymity and John Doe. *Network World*, 16, pp. 26 – 27.

Glasser, W.M., 1965, 'Learning to succeed through a higher self-concept'. In *Reality Therapy*, (New York: Harper & Row) pp. 9 – 10.

Hastak, M., Mazis, M.B. and Morris, L.A., 2001, The role of consumer surveys in public policy decision making. *Journal of Public Policy and Marketing*, 20, pp. 170 – 185.

Hoffman, D.L., Novak, T.P. and Peralta, M., 1999, Building consumer trust online. *Communications of the ACM*, 42, pp. 80 – 85.

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

Hofstede, G., 1991, *Cultures and Organizations* (London: McGraw-Hill).

Kohlberg, L. and Turiel, E. (Ed.), 1971, 'Moral Development and Moral Education'. In G. Lesser (Ed), *Psychology and Educational Practice*, (Glenview, IL: Scott Foreman). Scott Foresman.

Lee, A.S., 1991, Integrating positivist and interpretive approaches to organizational research. *Organizational Science*, 2, pp. 342 – 365.

Liu, C., Marchewka, J.T. and Ku, C., 2004, American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce. *Journal of Global Information Management*, 12, pp. 18 – 40.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C., 2005, Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information and Management*, 42, pp. 289 – 304.

Malin, B. and Sweeney, L., 2004, How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems. *Journal of Biomedical Informatics*, 37, pp. 179 – 192.

Mason, R.O., Mason, F.M. and Culnan, M.J., 1995, *Ethics of Information Management* (Thousand Oaks, CA: Sage Publications, Inc.).

McColl Jr., H.L., 2000, Communities of trust: the issue of privacy. *Vital Speeches of the Day*, 66, pp. 557 – 560.

McDougall, W., 1928, *An Introduction to Social Psychology* (London: Methuen & Co.).

Mehrabian, A. and Epstein, N., 1972, A measure of emotional empathy. *Journal of Personality*, 40, pp. 525 – 543.

Metcalfe, B., 1994, New technologies provide better combinations of privacy and anonymity. *InfoWord*, 16, pp. 65 – 67.

Milne, G.R. and Culnan, M.J., 2002, Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998 – 2001 U.S. Web surveys. *The Information Society*, 18, pp. 345 – 359.

Mühlenfeld, H., 2005, Differences between 'talking about' and 'admitting' sensitive behaviour in anonymous and non-anonymous Web-based interviews. *Computers in Human Behavior*, 21, pp. 993 – 1003.

Pederson, D.M., 1997, Psychological functions of privacy. *Journal of Environmental Psychology*, 17, pp. 147 – 156.

Pottie, G., 2004, Privacy in the global e-village. *Communications of the ACM*, 47, pp. 21 – 23.

Preston, R., 2001, It's up to e-business to 'get over' privacy issue. *InternetWeek*, 9.

Rachels, J., 1975, Why privacy is important. *Philosophy and Public Affairs*, 4, pp. 323 – 333.

Rosenberg, M., 1965, *Society and Me Adolescent Self-Image* (Princeton, NJ: Princeton University Press).

Rutter, D.R. and Stephenson, G.M., 1979, The role of visual communication in social interaction. *Current Anthropology*, 20, pp. 124 – 125.

Sheehan, K.B. and Hoy, M.G., 2000, Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19, pp. 62 – 73.

Smith, H.J., Milberg, S.J. and Kallman, E.A., 1995, *Privacy Practices around the World: An Empirical Study* (Washington, DC: Georgetown University).

Smith, H.J., Milberg, S.J. and Burke, S.J., 1996, Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20, pp. 167 – 196.

Stegeman, L., 2004, Who's afraid of the big bad wolf? Retrieved January 3, 2005, from http://www.bigresearch.com/news/big102604.htm

Stewart, B., 1996, Privacy impact assessments. *Privacy Law & Policy Reporter* 3, 4 (July 1996) 61 – 64. Retrieved October 31, 2006 from http://www.austlii.edu.au/au/journals/PLPR/1996/39.html

Tanis, M. and Postmes, T., 2007, Two faces of anonymity: paradoxical effects of cues to identity in CMC. *Computers in Human Behavior*, 23, pp. 955 – 970.

Tidwell, L.C. and Walther, J.B., 2002, Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: getting to know one another a bit at a time. *Human Communication Research*, 28, pp. 317 – 348.

Tourangeau, R., Couper, M.P. and Steiger, D.M., 2003, Humanizing self-administered surveys: experiments on social presence in Web and IVR surveys. *Computers in Human Behavior*, 19, pp. 1 – 24.

Turner, E.C. and Dasgupta, S., 2003, Privacy on the Web: an Examination of user concerns, technology, and implications for business organizations and individuals. *Information Systems Management*, 20, 8 – 18.

Turner, C.F., Forsyth, B.H., O'Reily, J.M., Cooley, P.C., Smith, T.K., Rogers, S.M. and Miller, H.G. (Ed.), 1998, *Automated Self-interviewing and the Survey Measurement of Sensitive Behaviors* (New York: Wiley).

Uslaner, E.M., 2002, *The Moral Foundations of Trust* (New York: Cambridge University Press).

Wallace, P., 1999, *The Psychology of the Internet* (New York: Cambridge University Press).

Walther, J.B., Slovacek, C.L. and Tidwell, L.C., 2001, Is a picture worth a thousand words? photographic images in long-term and short-term computer-mediated communication. *Communication Research*, 28, pp. 105 – 134.

Watson, D. and Friend, R., 1969, Measurement of social evaluative anxiety. *Journal of Consulting and Clinical Psychology*, 33, pp. 448 – 458.

Westin, A., 1967, *Privacy and Freedom* (New York: Quadrangle Books).

Westin, A.F. and Baker, M.A., 1972, *Databanks in a Free Society* (New York: Quadrangle Books).