Repositorio Institucional de la Universidad Autónoma de Madrid

https://repositorio.uam.es

Esta es la **versión de autor** del artículo publicado en:

This is an **author produced version** of a paper published in:

Journal of Advertising 38 (4) (2009): 63-77

DOI: http://dx.doi.org/10.2753/JOA0091-3367380405

© 2009 American Academy of Advertising. All rights reserved.

El acceso a la versión del editor puede requerir la suscripción del recurso
Access to the published version may require subscription

CONSUMER PRIVACY CONCERNS AND PREFERENCE FOR DEGREE OFREGULATORYCONTROL

A Study of Mobile Advertising in Japan

Shintaro Okazaki, Hairong Li, and Morikazu Hirose

ABSTRACT: This study explores the consequences of consumers' privacy concerns in the context of mobile advertising. Drawing on social contraer theory, the proposed research model connects a series of psychological factors (prior negative experience, information privacy concerns, perceived ubiquiry, trust, and perceived risk) and preference for degree of regulatory control. Data from a survey of 51O mobile phone users in Japan show that mobile users with prior negative experiences with information disclosure possess elevated privacy concerns and perceive stronger risk, which leads them to prefer stricter regulatory controls in mobile advertising. Both perceived ubiquity and sensitivity of the information request further the negative impact of privacy concerns on trust. No such effect occurs for the impact of privacy concerns on perceived risk, however. The authors discuss sorne theoretical and managerial implications.

Consumer privacy concerns with respect to mobile advertising have become an important issue for policymakers, trade groups, and consumer advocates as unfair information practices continue to escalare in many countries. In the United States, unsolicited messages or spam increased by 38% from 2006 to 2007 and was expected to increase by 50% more to l.5 million messages in 2008 (Cloudmark 2008). Sorne spam messages request mobile users to provide personal information, including their credit card numbers, or attempt to infiltrare mobile devices with virus programs by asking users to register for services (CNET.co.uk 2006).

To alleviate consumers' concerns about these potential invasions, the mobile industry has implemented several self-regulations. For example, the Mobile Marketing Association recently revised its consumer best practices guidelines, including those regarding promotional content and marketing to children; it also expanded and clarified its guidelines for free, standard, and premium rate messaging, mobile Web, and interactive voice responses (Mobile Marketing Association 2008). The U.S. Federal Trade Commission (FTC) held a town hall meeting in May 2008 for business executives, consumer advocates, and scholars to explore issues of mobile privacy and consumer protection (Corbin 2008). InJapan, spam regulation violators may be sentenced to up to one year in prison and a fine of up to 1 million yen (approximately US$11, 135) (Ministry of Interna! Affairs and Communications 2008).

Despite these different regulatory measures, what makes the most effective type of regulation in terms of protecting consumer information privacy remains a topic of debate. To assess the appropriateness of different approaches, we might examine mobile users' preferences for the degree of regulatory control, because users influence both mobile service providers and regulatory government agencies. Therefore, this research explores the relationship between consumer privacy concerns in mobile advertising and their preference for three types of regulations: government regulation, industry self-regulation, and government and industry coregulation. Government regulation constitutes an authoritative and powerful exertion of government control (Rose 2006). With self-regulation, an industry-level organization sets and reinforces rules and standards relating to the conduct of firms and individuals in the industry, whereas coregulation refers to mixed systems that involve sorne type of government regulation of the self-regulation (Gupta and Lad 1983).

Furthermore, we employ social contraer theory as an overarching framework that connects the key study variables, including trust, perceived risk, and perceived ubiquity. Mobile

Shintaro Okazaki (Ph.D., Universidad Autónoma de Madrid) is an associate professor of marketing, College ofEconomics and Business Administration, Universidad Autónoma de Madrid.

Hairong Li (Ph.D., Michigan State University) is a professor of advertising, College ofCommunication Arts and Sciences, Michigan State University.

Morikazu Hirose (M.A., Waseda University) is an associate professor of marketing, Faculty of Business Administration, Tokyo Fuji University.

This research was funded by a grant from the Spanish Ministry of Science and lnnovation (National Plan for Research, Development and Innovation EC02008-0 1557) and the lnternational Communication Foundation inJapan. The authors thank the special issue editors and three anonymous reviewers for their insightful comments on a previous version of this manuscript.

users undergo different experiences with unfair information practices, especially in countries marked by widespread use of mobile phones, where mobile advertising has become a feature of everyday life. Users' experiences, especially their negative experiences in association with information disclosure, likely heighten their information privacy concerns, which may weaken their trust in mobile advertisers and increase their perceived risk of responding to mobile advertising. In turn, users' preferences may lean toward more strict forros of regulatory control in mobile advertisíng. Perceived ubiquity or flexibility in time and place plays pivota! roles in mobile-based communications, which may affect consumers' trust and perceived risk in a given environmental context. We integrare these factors into a causal model and test it using data from a survey of mobile users in Japan, one of the most advanced countries in terms of mobile phone adoption, where regulations on mobile advertising have been in place for severa! years. The findings shed unique light on the psychological processes that mobile phone users experience in developing their preferences for regulatory control.

LITERATURE AND HYPOTHESES

This study examines the impact of mobile users' privacy conceros on their preference for the degree of regulatory control using a psychological perspective that integrares the theories of social contraer, trust, and perceived risk. We therefore develop a conceptual model (see Figure 1), which also includes perceived ubiquity, because mobile phones can be used anywhere and anytime. We define perceived ubiquity as the user's perception of the mobile phone's usage flexibility in terms of time and place. Next, we review existing literature pertaining to the key concepts in the model and delineare the relationships among them.

Social Contraer Theory

To conceive of how society organizes in accordance with the mutually beneficia! principals of justice, social contraer theory provides a rationale for the historically important notion that legitimare state authority must be derived from the consent of the governed (Macneil 1974, 1980). Social contracts comprise a broad class of implied agreements by which people forro nations and maintain social arder. Thus, social contraer theory atrempts to explain why rational and impartial people voluntaríly give up their freedom of action in a natural state ("natural rights") to obtain the benefits provided by the formation of social structures (Macneil 1974).

According to this theory, the nature of a contraer evolves from four principals of society: specialization of labor, exchange, choice, and awareness of the future. As labor has become more specialized over time, persons and companies no longer produce for themselves everything they need to thrive; instead, they must depend on exchanges with others for produces and services. Exchanges that involve the promise of future benefits represent contracts. Furthermore, the level of choice that people and/or companies have among a range of exchanges reveals rhe extent of freedom they enjoy. Without awareness of the future, however, a contraer that defines such exchanges is not worth pursuing, because consciousness of the future determines the need for a contraer (Macneil1974).

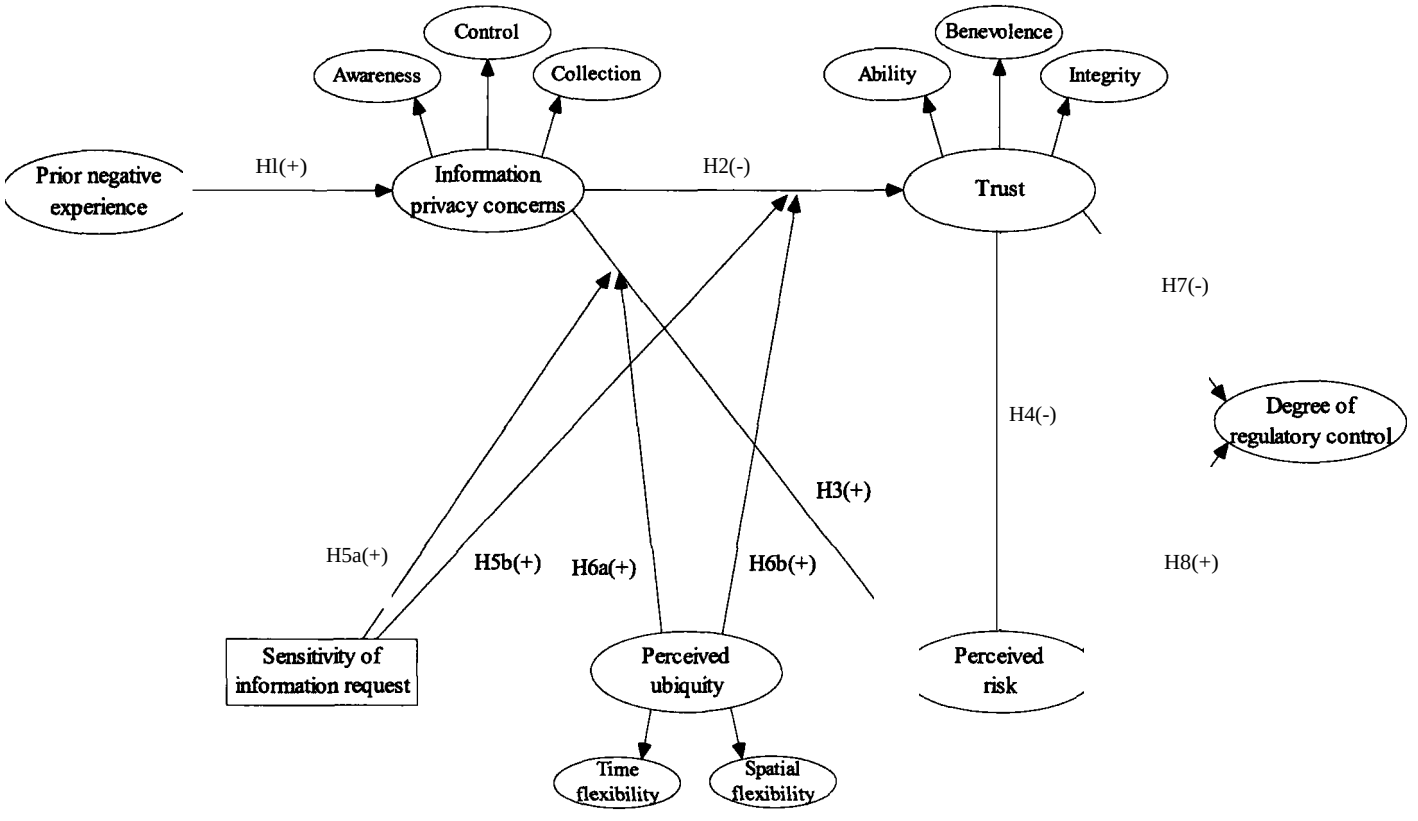
Macneil (1980) also argues that contracts entail a continuum, from discrete to relacional. Discrete contracts are short-term, single transactions between unrelated parties, whereas relational contracts involve long-term, dynamic transactions with related parties. These relationships are separare from the exchange of the goods. Therefore, in a marketing context, direct marketing requires social contracts, that is, implicit, noncommercial relationships characterized by multiple transactions between consumers and marketers (Milne and Gordon 1994). Consumers provide information in exchange for solicitations, but if marketers break from the expected pattern of behavior, consumers believe their rights have been violated (Milne and Gordon 1994).

To establish our theoretical framework, we view the relationships between mobile users and mobile advertisers as an implicit social contraer. When mobile users provide personal information in exchange for relevant services, they expect their rights to the information to be respected by users of that information. This belief essentially reflects the concept of trust, which we also integrare into our study context. In a similar fashion, when mobile advertisers collect users' information to provide services, users anticipare that the use of this information will not go beyond mutually accepted purposes. Users also perceive a certain risk in exchanging such information, however. Moreover, the behavioral consequences of information use should be governed by regulatory control mechanisms; users must determine their preference for government regulation, industry self-regulation, and government and industry coregulation. Because of information asymmetry, such that the identities of mobile users are known but the identities of mobile advertisers are unknown, especially in the case of spam, mobile users suffer more vulnerability in this implicit social contraer (Dinev and Hart 2004). Thus, the degree of regulatory control imposed should respect the preferences of mobile users, according to the social contraer perspective.

Information Privacy Concerns

The concept of information privacy deals with the rights of those people whose information is shared. Westin defines information privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent informar ion about them is communicated to oth-

FIGURE 1
Research Model of the Degree of Regulatory Control in Mobile Advertising



ers" (1967, p. 7). Information privacy becomes a prominent issue in computer-mediated communication, because the interactive process can collect significant amounts of personal information and store it indefinitely for later use.

Organizationalliterature offers severa! theories about consumers' information privacy concerns. Smith, Milberg, and Burke (1996) develop a 15-item scale that measures informadon privacy concerns on four dimensions: improper access to personal information, collection, errors, and unauthorized secondary use. The scale has received empirical validation in severa! offline contexts (Milberg, Smith, and Burke 2000; Rose 2006; Stewart and Segars 2002). Furthermore, drawing in part on Smith, Milberg, and Burke's (1996) scale, Malhotra, Kim, and Agarwal (2004) develop an extended scale to measure Internet users' information privacy concerns and identify lnternet-specific dimensions of privacy, distinct from those surrounding traditional marketing. Also on the basis of social contraer theory, they propase three factors: collection, control, and awareness of privacy practices.

Collection entails the degree to which a person worries about the amount of data possessed by others, relative to the value of the benefits received. This factor derives from the social contraer principal of distributive justice, which assumes that in an equitable exchange, consumers relinquish sorne information in return for something of value, after evaluating the costs and benefits associated with that particular transaction. Thus, people are reluctant to release personal information if they expect negative outcomes. Control refers to the degree to which a person can exercise the freedom to accept or reject the process or decision outcome related to his or her personal information. This construct derives from the principle of procedural justice, which states that consumers want to exercise process control and effect changes in organizational policies that they find objectionable. Finally, awareness of privacy practices is the degree to which a consumer worries about his or her awareness of organizational information privacy practices. This construct is based on two types of justice: interactional and informational. In the former perspective, violating the transparency and propriety ideals of information leads to decreased perceptions of fairness, whereas according to the latter perspective, perceptions offairness increase with the specificity of information used to provide a justification. In two empirical studies, Malhotra, Kim, and Agarwal (2004) find empirical support for this scale's reliability and validity.

In the context of mobile advertising, information privacy usually is protected by mandatory opt-in and opt-out systems,

associated with any subscription to message-based promotions. Barwise and Strong (2002), Tsang, Ho, and Lian (2004), and Rettie, Grandcolas, and Deakins (2005) investigare consumers' acceptance of permission-based advertising in the form ofSMS (short message service); unknown messages sent to consumers likely annoy recipients and appear to be spam (Okazaki and Taylor 2008). Although Barwise and Strong's (2002) findings are somewhat optimistic, mobile advertising practices suggest that a permission system alone cannot ensure consumers' confidence, because as "an individual's subjective views of fairness within the context of information privacy" (Malhotra, Kim, and Agarwal 2004, p. 337), information privacy concerns arise whenever users suspect that their personal information rights have been violated.

Prior Negative Experience

Internet advertising researchers establish that prior negative experience with Internet advertising prompts users to avoid Internet advertising (Cho and Cheon 2004). Similarly, mobile users' experience with information disclosure can be either positive or negative. From a social contraer perspective, a failure to meet their expectations induces negative experiences. Even if mobile users have mostly positive experiences, a single event that induces a negative experience can heighten privacy concerns. For example, mobile users who receive personalized messages from unknown advertisers may suspect their personal information is being abused. In addition, most users likely have negative experiences, because as much as 80% of e-mail or SMS-based advertising consists of spam (Cloudmark 2008), and fraudulent acts such as "smishing" or "phishing" attacks are prevalent (CNET.co.uk 2006). Such experiences can form an episodic memory, which elicits specific feelings (Hawkins, Best, and Coney 2001) and heightens information privacy concerns. Therefore, we hypothesize:

H 1: Prior negative experience inpersonal information disclosure increases mobile users' information privacy concerns.

Trust and Perceived Risk

Trust and perceived risk are two salient beliefs in information privacy contexts (Miyazaki and Fernandez 2000). Trust provides the foundation for a social contraer. As Golembiewski and McConkie state, "There is no single variable which so thoroughly influences interpersonal and group behavior as does trust" (1975, p. 131). When parties engage in a contractual relationship, one party must assume that the other will take responsibility for its promises. Moorman, Deshpandé, and Zaltman (1993) conceptualize trust as a willingness to reply to an exchange partner in whom one has confidence, grounded in Rotter's (1971) classic definition of trust as one party's general expectation that it can rely on another.

In the e-commerce context, the relationships between privacy concerns, privacy seals, privacy policy, and trust have been well studied (Bart et al. 2005; Fuller, Serva, and Benamati 2007; Jarvenpaa, Tractinsky, and Saarinen 1999; Rifon, LaRose, and Choi 2005; Stewart 2003). Metzger (2004) finds that users' privacy concerns negatively affect their trust in Web sites, and Schoenbachler and Gordon (2002) explore the role of trust in consumers' willingness to provide the information necessary to build a strong relationship with marketers. In Sheehan and Hoy's (1999) study, as concern about privacy increases, users register for Web sites less frequently and provide incomplete information, possibly because they have less trust in the Web site. That is, trust becomes manifest in the willingness of a party to be vulnerable to the actions of another, based on the expectation that the other will perform a particular action important to the truster, irrespective of its ability to monitor or control that other party (Mayer, Davis, and Schoorman 1995).

The impact of privacy concerns on trust in an exchange relationship should be greater in mobile communications, because mobile phones provide a personal medium. They are more intimare to users, in that they are rarely shared and generally exclusively employed by individual users. Thus, mobile phone users may be more concerned with the privacy of information pertaining to their phone numbers, usage, and personal background. From a social contraer perspecrive, the privacy concerns of mobile users may cast doubt on mobile advertisers' commitment to fair use of personal information, which may diminish their trust in mobile advertisers, as Metzger (2004) finds. Mobile users also should trust a mobile advertiser less if they are concerned that their personal information has not been used fairly. We thus anticípate that consumers who possess prior negative experience and elevated privacy concerns likely express lower levels of trust.

H2: Information privacy concerns decrease mobile users' trust in mobile advertising.

If mobile users also believe that advertisers choose not to fulfill their implicit or explicit obligations, they may feel that they are risking sorne of their rights. Marketing literature conceptualizes perceived risk as beliefs about uncertainty and consequences (Pavlou 2003). We adopt this concept and further define perceived risk in mobile advertising as the extent to which users are uncertain about the negative consequences of opening, reading, or responding to mobile advertising. When mobile users are concerned about their information privacy, they likely perceive an increase in the likelihood of negative consequences resulting from their response to mobile advertising. Thus, it is reasonable to posit that information privacy concerns may drive perceived risk in mobile advertising:

H3: lnformation privacy concerns increase mobile users' perceived risk in mobile advertising.

Trust and perceived risk function in tandem to explain consumer behavior in uncertain environments. Trust in advertisers depends on many various factors in e-commerce, including overall satisfaction, lack of utility, incentives in ads, and privacy concerns (Pavlou 2003). Once established, trust plays a unique role, such that higher levels of trust can reduce the level of perceived risk. Consumers who trust an advertiser are less likely to foresee negative consequences of dealing with that advertiser, but when potential risk is higher, trust becomes an even more important determinant of risk-taking behavior. This relationship berween trust and perceived risk has been documented in various srudies *(J*arvenpaa, Tractinsky, and Saarinen 1999; Pavlou 2003). Camerer further recognizes: "Trust must be risky. Trustworthiness must also go against the trustee's self-interest, to test whether people are willing to sacrifice to satisfy moral obligation" (2003, p. 85). The relationship between trust and perceived risk in mobile communication resembles that in e-commerce (Okazaki, Katsukura, and Nishiyama 2007). Therefore, we hypothesize:

H4: Trust decreases mobile users' perceived risk in mobile advertising.

Sensitivity of the Information Request

Another issue related to privacy concerns is the sensitivity of the information requested by the marketers. Malhotra, Kim, and Agarwal (2004) find that a request for more sensitive information in an e-commerce setting reduces trust and increases perceived risk, because the request makes consumers more cautious and suspicious about a marketer. However, these researchers do not address whether a request for more sensitive information results in heightened consumer concerns about marketers' unfair information practice. That is, consurners may be more concerned when asked about their name and household income rhan about rheir brand preferences. Thus, more sensitive informarion requests may lead ro grearer privacy concerns, and we consider the moderaring effect of informarion sensitivity on rhe impact of privacy concerns on trust and perceived risk in a mobile advertising context. Specifically, we postulare that when mobile advertisers solicit more sensitive information, the strength of relationships among information privacy concerns, trust, and perceived risk should change, as follows:

H5a: The sensitivity of an information request moderates the relationship between information privacy concerns and trust; specifically, the greater the sensitivity of the information request, the stronger the effect of information privacy concerns on trust.

H5b: The sensitivity of an information request moderates the relationship between information privacy concerns and perceived risk; specifically, the greater the sensitivity of the information request, the stronger the elfect of information privacy concerns on perceived risk.

Perceived Ubiquity

Ubiquity-or rhe usage flexibility of time and locarion-represents a unique fearure of mobile phones (Barnes and Huff2003). Hagerstrand (1975) argues that three time-space consrraints characterize information technology: coupling, which requires the user's presence ata specific time and place; capability, which refers to the user's resources and ability to overcome spatial separarion at a specific moment; and the time-space zones, which limit access to specific schedules or hours of service. Mobile ubiquity enables users to overcome all three constraints.

The perceived level of ubiquity may moderare the influence of informarion privacy concerns on trust and perceived risk. For example, use flexibility in terms of location increases when location-based services in mobile commerce become available for GPS (global positioning system)-enabled phones. Thus, mobile advertisers can now target mobile users with rhe addirional parameter oflocation. Although location-based services may offer benefits to mobile users, rhe concerns they provoke pertaining ro user privacy are significant (Chen, Ross, and Huang 2008; Reedy 2008). Thus, we speculate that the perceived ubiquity of mobile phones increases anxiety about the collection of personal informarion without users' awareness. Such worries likely enhance rhe impact of privacy concerns on trust in mobile advertising. In a similar fashion, rhe substantial trackabiliry associated with the use of location-based services may inrensify the influence of informarion privacy concerns on unforeseen abuses and thus increase perceived risk. Formally:

H6a: Perceived ubiquity moderates the relationship between information privacy concerns and trust; specifically, the greater the perceived ubiquity, the stronger the effect of information privacy concerns on trust.

H6b: Perceived ubiquity moderates the relationship between information privacy concerns and perceived risk; specifically, the greater the perceived ubiquity, the stronger the effect of information privacy concerns on perceived risk.

Degree of Regulatory Control

Rose (2006) proposes six levels of regulatory control: no policy, self-help, voluntary control, data commissioner, licensing, and registration. Voluntary control is synonymous with self-regulation, by which firms self-regulate by developing their own policies and monitoring their compliance. The data commissioner stage parallels coregulation, such rhat a separare government agency audits information processing operations and provides advice to both legislators and prívate organizations about information handling. Registration is rhe strictest option; organizations must license their collection of personal information with a government agency.

On the basis ofRose's (2006) scheme and related literarure, we focus on three types of regulatory control in mobile advertising: government regulation, industry self-regulation, and government and industry coregulation. In general, government regulation is stricter than government and industry coregulation, which is stricter than industry self-regulation. We posit that mobile users' perceived risk affects their preferences for the degree of regulatory control in mobile advertising. If a privacy problem arises because of people's inability to control their personal information, they may prefer centrally administered regulations. If users perceive the problem as a question of the legal rights of individuals with respect to the availability and protection of their personal information against both public and privare violations, they instead may prefer coregulation. Because a social contraer is based on trust, we assume that if mobile advertisers comply with the social norms of fair information practices and deliver trustworthy information, mobile users will be generous in granting advertisers the procedural rights to implement self-regulation. Thus, we believe that higher levels of trust in mobile advertising should be associated with a preference for less strict levels of regulatory control.

H7: Trust causes mobile users to prefer less strict regulatory controls in mobile advertising.

However, one of the consequences of perceived risk may be a preference for stricter regulatory controls. The prevalence of problems such as spam and phishing in general may make mobile users, who are uneasy about unsafe information practices, demand stricter regulatory control. Thus, we postulare that when users perceive mobile advertising as more risky, they are likely to prefer stricter regulatory controls. Hence:

HS: Perceived risk causes mobile users to prefer more strict regulatory controls in mobile advertising.

METHOD

Japan serves as the site for this study for several reasons. In particular, it has one of the highest mobile phone penetration rates: In 2008, there were 107.96 million mobile subscribers in the Japanese market, and subscribers to 3G services accounted for 83.8% (Business Monitor International 2008). Beginning in 2005, more Japanese users accessed Web sites from mobile phones than from PCs (Ministry of lnternal Affairs and Communications 2007), and various new functions have been integrated in the latest models of mobile phones, including GPS, QR (Quick Response) code, digital terrestrial television, electronic money, and credit cards, which make mobile phones seem like a dream medium for advertisers (Dou and Li 2008).

As a result of the growth of mobile advertising, unfair information practices have been on the rise. For example, a malicious code infiltrated the Japanese mobile Internet ("i-mode") system in 2000. This code sent numerous wireless users a message with a hypertext link that, when clicked and without the user's awareness, dialed 110-theJapanese emergency number, equivalent to 911 in North America (Trend Micro 2001). In 2001, abuse by an Internet dating service sent more than 900,000 text messages, including 170,000 undeliverable messages, to i-mode users in an hour (Petty 2003). The industry soon established its own interest group, Spam Mail Measures Association, to counter spammers, and government encouraged the mobile phone carriers to cooperare with one another, while strengthening the Act on the Regulation ofTransmission ofSpecified Electronic Mail, in 2005, by extending the existing scope to treat a person as a spammer and SMS (short messaging service) as e-mail *(Nikkei Sangyo Shinbun* 2006). Japan thus has various types of regulation designed to protect the information privacy of mobile users. These developments make Japan an ideal site for investigating how mobile users' experience affect their concerns about privacy, as well as their preferences for the degree of regulatory control over mobile advertising.

Data Collection

We test our hypotheses using data from a survey of mobile users in Japan during spring 2008. A professional research firm recruited participants from its online panel. A filter question ("Do you regularly access the Internet with your mobile phone or personal handy phone, for e-mailing, browsing news, social networking sites and/or blogs, music and/or game downloads, shopping, etc.?") identified 510 participants who regularly use their mobile phones to access the Internet. The demographic distribution approximately marches that of the general Japanese population. We adopt a between-subjects quasi-experimental design, in which the participants are randomly divided into high- and low-risk scenario groups (i.e., 255 respondents for each scenario), in equal proportion by gender and age. In Table 1, we summarize the respondents' profiles in terms of age, gender, and occupation. To ensure respondents' experience with mobile devices, we calculare the means for mobile usage level (i.e., time) and mobile e-mail frequency; the Pearson correlation is statistically different from O at $p < .001$, which confirms that these respondents engage in an appropriate level of mobile usage.

Measures

The survey instrument consists of two parts. In the first part, we request demographic information, mobile device usage levels, outgoing mobile e-mail frequency, and descriptions of prior negative experiences. The second part includes two mobile advertising scenarios with high- and low-risk siruations,

TABLE
Respondents' Profiles

Demographics	More sensitive information request scenario (n = 255)	Less sensitive information request scenario (n = 255)	Total sample (N= 510)
Gender			
Male	51.37	51.37	51.37
Female	48.63	48.63	48.63
Age			
20-29	22.35	22.35	22.35
30-39	27.84	27.84	27.84
40-49	23.92	23.92	23.92
50-59	25.88	25.88	25.88
Occupations			
Executive/managerial	4.71	4.31	4.51
Administrative/clerical	43.14	40.39	41.76
Self-employed	10.98	9.02	10.00
Part-time workers	8.24	13.33	10.78
Housewives	19.22	19.61	19.41
Students	2.35	3.92	3.14
Unemployed	5.10	5.10	5.10
Others	6.27	4.31	5.29

as well as the measures we describe in the following section. As a pretest, 135 business majors in three large metropolitan universities in Tokyo completed the instrument during class meetings of a marketing course. The results showed that sorne of the respondents had trouble understanding two items, so we revised the wording of these items accordingly. The Cronbach's as exceed the reliability level of .80 for all constructs (Nunnally 1978).

Most of the measures we use are adapted from published srudies. For prior negative experience, we adapt the scale from Cho and Cheon (2004). We conceptualize perceived ubiquity as a second-order construct consisting of time flexibility (three items) and spatial flexibility (three items). For time flexibility, we adapt an efficiency scale from Mathwick, Malhotra, and Rigdon (2001). For spatial flexibility, we propase severa! original items based on the qualitative study. The mobile users' information privacy concerns scale comes from Malhotra, Kim, and Agarwal (2004), specified as a second-order construct consisting of awareness (three items), control (three items), and collection (four items). The trust scale, adopted from Schlosser, White, and Lloyd (2006), represents a second-order construct of ability (five items), benevolence (five items), and integrity (five items). Perceived risk (five items) also comes from Malhotra, Kim, and Agarwal (2004). We measure these multiple-item constructs using seven-point Likert-type scales with anchors of "strongly disagree" and "strongly agree." Finally, we measure regulatory control expectations with a categorical variable, using alead of"I think information privacy in mobile advertising can be best protected and controlled by …" Respondents choose one of the following responses: (1) industry self-regulatíons, (2) both or coregulation, and (3) governmental regulations. We also add an option, "1 don't know/cannot answer," to avoid a forced choice. The Appendix lists all the questionnaire items.

Scenario Creation

To investigare how the sensitivity of information requested by advertisers affects consumers' reactions to privacy threats, we employ a quasi-experimental, between-subjects design with a scenario-creation method (Malhotra, Kim, and Agarwal2004; Webster and Trevino 1995). Specifically, we creare two types of scenarios according to the sensitivity of the personal information requested. In the less sensitive scenario, respondents must provide their gender, age, and zip code to participare in a music-download sweepstake. In the more sensitive scenario, they must provide additional information, including their name, address, and household income. People generally perceive financia! information as more sensitive than their personal preferences (Sheehan and Hoy 2000), especially in Japan. We assume our respondents already have opted-in for an e-mail newsletter subscription, which is realistic, because it is very unlíkely that consumers would respond to or even open an e-mail ad from a completely unknown advertiser.

Respondents see only one of the two scenarios; a pretest confirmed the difference berween rhe two levels of sensitiviry in the information request ($t = 5.23, p < .001$).

ANALYSIS AND RESULTS

Partial Least Squares

We use partialleast squares (PLS), specifically Smart PLS version 2.0M3 (Ringle, Wende, and Alexander 2005), for rhree main reasons. First, PLS is robust across different scale rypes, including quasi-metric or nominal scales (Chin 1998; Hulland 1999), which is appropriate for our dependent variable, degree of regulatory control, which we measure with an ordinal scale. Second, PLS does not require stringent assumptions about the distribution of latent or manifest variables. Thus, the data may be non-normal or skewed, and the observations may be interrelared (Falk and Miller 1992). Third, PLS is a prediction-oriented method, which is appropriate for testing a set of hypotheses based on rheories.

Measurement Model Assessment

We evaluare the measurement model following generally accepted guidelines (Chin 1998). After pooling the data from the two scenarios, we apply a bootstrapping method with 500 cases (sample size 200) to calculare t-values. We assess model fit in light of the estimation of individual itero reliability, retaining only those items that score higher than .70 (Hair et al. 2006). This guideline ensures more shared variance between the construct and its measure than error variance (Diamantopoulos and Winklhofer 2001). Five of the items do not meer this criterion, and we eliminare them from further analysis.

We summarize the descriptive statistics and quality indicatoes in Table 2. To determine the level of interna! consistency and convergent validity, we calculare composite reliability (CR) and average variance extracted (AVE) (Hair et al. 2006). With respect to the CR, all constructs return values higher than the suggested threshold value of .07 (Bagozzi and Yi 1988), in support of interna! consistency. Furthermore, for all constructs, the AVE is greater than the suggested benchmark of .50 (Hair et al. 2006), in support of good convergent validity. Finally, the predictive power of a PLS model can be measured by Stone-Geisser criterion (Q^2) (Chin 1998). If the model outperforms the alternative model, this index should be positive and less than 1; we find support for the predictive power of all constructs.

Next, we assess discriminant validity using the latent constructs correlations matrix, in which the square roots of the AVE appear along the diagonal, and the correlations between the constructs appear in the lower left, off-diagonal elements. Discriminant validity exists if the diagonal elements (square-root AVE) are greater than the off-diagonal elements in the same row and column (Hair et al. 2006). The combinations for our study meet this condition, with the exception of 13 cases, most of which relate to the correlations between second-order and first-order factors. These points should cause little concern, because the constructs are conceptualized as second-order models and thus are highly correlated. Therefore, we establish at least reasonable discriminant validity.

Hypotheses Testing

To test the hypothesized relationships among the proposed constructs, we use PLS, and we summarize the results in Table 3. With H 1, we address the direct effects of prior negative experiences on information privacy concerns and find a modest but statistically significant structural path ($\gamma = .18$, $p < .001$).

We also postulare sorne consequences of information privacy concerns in terms of trust and perceived risk. Our results indicare that the path from information privacy concerns to trust is negative and statistically significant ($\gamma = -.34$, $p < .001$), in support ofH2, and that the path from information privacy concerns to perceived risk reveals a highly positive and significant standardized coefficient ($\gamma = .74, p < .001$), in support of H3. In H4, we posit that trust negatively affects perceived risk, and the results indicare that this path is negative and statistically significant ($\gamma = -.17, p < .001$).

In H5a and H5b, we posit moderating effects of the level of sensitivity of the information request on the relationships between information privacy concerns and trust and between information privacy concerns and perceived risk, respective!y. Therefore, we compare the strength of the path coefficients between the two levels of sensitivity in information request. As suggested by Chin (1998), we run separare PLS models for each sample, rhen calculare the t-values for the differences in their path coefficients. The results indicare that the difference is statistically significant with regard ro the relationship between information privacy concerns and trust ($t = 4.45$, $p < .001$), but not for the relationship berween information privacy concerns and perceived risk. Thus, H5a receives support, but H5b does not.

We also predict a moderation effect of perceived ubiquity on the relationships berween information privacy concerns and trust and perceived risk. [1] To test H6a and H6b, we employ a product indicator approach, as proposed by Chin, Marcolin, and Newsred (2003). The results confirm that the moderation effect for the relationship between information privacy conceros and trust is statistically significant ($\gamma = -.13, p < .001$). Furthermore, we find significant main effects for the predictor (information privacy concerns) and the moderator (perceived ubiquity) on the effects between information privacy concerns

TABLE
Means, Standard Deviations, and Quality lndicators (N = 51 O)

Construct	*M*	SO	a	CR	AVE	Ql
Prior negative experience	4.25	1.86	.91	.94	.85	.65
lnformatian privacy cancerns			.92	.93	.58	.48
Awareness	6.10	1.00	.90	.94	.83	.49
Control	5.52	1.07	.90	.93	.77	.60
Collection	5.75	1.12	.74	.85	.66	.32
Trust			.94	.95	.67	.58
Ability	3.56	1.30	.88	.91	.67	.51
Benevolence	2.97	1.33	.93	.95	.78	.63
lntegrity	2.95	1.16	.83	.90	.70	.61
Perceived ubiquity			.86	.89	.59	.42
Time flexibility	4.49	1.51	.80	.88	.71	.41
Spatial flexibility	4.78	1.38	.79	.88	.70	.39
Perceived risk	5.67	1.10	.76	.89	.73	.63

Notes: a= Cronbach's a; CR = composite reliability; AVE =average variance extracted; Q^2 = Stone-Geisser criterion.

Degree of regulatory control is excluded because it is a single indicator.

TABLE 3
Hypotheses Testing by PLS

Hypotheses		Method	Statistics	Results
H 1	Prior negative experience in personal information disclosure increases mobile users' information privacy concerns.	Path coefficient•	= .18*	Supported
H2	lnformation privacy concerns decrease mobile users' trust in mobile advertising.	Path coefficientb	= -.34*	Supported
H3	lnformation privacy concerns increase mobile users' perceived risk in mobile advertising.	Path coefficient	= .74*	Supported
H4	Trust decreases mobile users' perceived risk in mobile advertising.	Path coefficient	= -.17*	Supported
H5a	The greater the sensitivity of the information request, the stronger the effect of information privacy concerns on trust.	Multigroup comparison	t = 4.45*	Supported
HSb	The greater the sensitivity of the information request, the stronger the effect of information privacy concerns on perceived risk.	Multigroup comparison	*n.s.*	Not supported
H6a	The greater the perceived ubiquity, the stronger the effect of information privacy concerns on trust.	Product indicator approach	= -.13*	Supported
H6b	The greater the perceived ubiquity, the stronger the effect of information privacy concerns on perceived risk.	Product indicator approach	*n.s.*	Not supported
H7	Trust causes mobile users to prefer less strict regulatory controls in mobile advertising.	Path coefficient	*n.s.*	Not supported
H8	Perceived risk causes mobile users to prefer more strict regulatory controls in mobile advertising.	Path coefficient	= .17*	Supported

Note: PLS = partialleast squares.

'The paths from information privacy concerns to awareness, control, and collection are al! statistically significant atp < .001, wirh srandardized coefficienrs of .86, .90, and .80, respective!y.

b The paths from trust to abiliry, benevolence, and inregriry are al! sratisrically significanr arp < .001, wirh srandardized coefficients of .94, .96, and .86, respectively.

*p < .001; *n.s.* = nonsignificanr.

and trust(= -.32, p < .001) and between perceived ubiquity and trust(= .22, p < .001). However, the moderation effect of perceived ubiquity on the relationship between information privacy concerns and perceived risk is negligible and insignificant. Thus, we find support for H6a but not for H6b.

Finally, we hypothesize that trust and perceived risk provide important predictors of mobile users' preference for the degree of regulatory control. Specifically, in H7, we predict that higher trust creares preferences for less strict regulatory control, and in H8, we posit that higher perceived risk prompts a desire for stricter regulatory controls. The effect of trust is negative but not significant, whereas the path from perceived risk to mobile users' preference for the degree of regulatory control is modestly positive and statistically significant (= .17, p < .001), in support ofH8.

SUMMARY AND DISCUSSION

This study examines the impact of severa! psychological factors on mobile users' preference for the degree of regulatory control in mobile advertising in Japan. It develops a conceptual model in light of the perspectives of social contraer, trust, and perceived risk. Seven of the 10 proposed hypotheses receive support. As a first attempt to investigare mobile users' preferences for the degree of regulatory control in mobile advertising, this study provides severa! theoretical and policy implications.

Theoretical Implications

We expand the information privacy concerns-trust-risk model developed by Malhotra, Kim, and Agarwal (2004) in an e-commerce setting to the context of mobile advertising by adding and establishing relationships among severa! new concepts, including prior negative experience, perceived ubiquity, information sensitivity, and preference for regulatory control. We conceptualize the relationships among these variables primarily on the basis of social contraer theory, which better captures the essence of information exchange as a social contraer relationship (Milne and Gordon 1994). The key outcome of our study is a causal model that empirically links prior negative experience, privacy concerns, perceived risk, and preference for stricter regulatory control. This model is certainly relevant for legal research into mobile advertising regulation, as far as mobile users are concerned.

We empirically establish a solid causal relationship between privacy concerns and perceived risk, although the link between privacy concerns and trust is modest, and trust has only a minor effect on perceived risk. Furthermore, contrary to our prediction, trust has no direct impact on preference for regulatory control. The reason for this is that trust may be more advertiser-specific, such that mobile users trust certain individual advertisers but not others. A general measure of trust in mobile advertisers thus may not have been as sensitive as we expected, which would result in these unforeseen outcomes. In contrast, perceived risk does not appear to be advertiser-specific; any advertiser that abuses users' personal information may raise mobile users' concerns. This general perception demonstrates the strong overall impact of risk on preferences for regulatory control (Sutherland 2007). However, trust should not be considered trivial in the model, because its relationship with perceived risk plays a key role. That is, privacy concerns reduce trust, which in turn increases perceived risk.

The results regarding the moderating role of the two new variables we propose-perceived ubiquity and sensitivity of the information request-are mixed. We include perceived ubiquity in the model because mobile phones can be used anywhere and anytime. The results indicare that its moderating role is significant for trust but not perceived risk. It seems that the magnitude of the impact of perceived ubiquity may depend on the strength of the relationship that it sets to modify. That is, perceived ubiquity plays a significant moderating role because the relationship between privacy concerns and trust is weak. In contrast, it plays an insignificant role because the relationship between privacy concerns and perceived risk is strong. In a similar fashion, the sensitivity of the information request fails to register a significant impact on the relationship between privacy concerns and perceived risk. Again, we speculate that such insignificance may be due to the strength of the relationship between privacy concerns and perceived risk. These mixed results are interesting and deserve further empirical investigation, as perceived ubiquity and sensitivity of the information request emerge as important factors in mobile advertising.

Policy Implications

This study provides mobile advertisers with insights they might use to safeguard themselves against regulatory control. The most important implication states that, from a social contraer perspective, users maintain rights over information about themselves; when they believe these rights are violated, they are reluctant to disclose personal information, will not respond to advertising offers, and may even seek stricter regulatory control over mobile advertising. Mobile advertisers therefore must respect users' information rights, because their failure to establish fair and relevant social contracts may ereate insurmountable obstacles to the success of promotional campaigns.

The varied impacts of trust and perceived risk on preference for regulatory control suggest that mobile advertisers may need to work both individually and together as an industry to address mobile users' privacy concerns. Individual mobile

advertisers should strive to establish trust among mobile users, whereas the industry as a whole should endeavor to reduce mobile users' perceived risk, which is a grave factor that induces preference for stricter regulatory controls. Mobile advertisers must make greater efforts in various ways to address privacy concerns.

Mobile marketers should also strengthen their spam blocking systems. Here, the notion of spam may include any criminally punishable deceptive communication by commercial parties. Industry data seem to indicare that current measures fail to salve the problem, as spammers continue ro invent other fraudulent methods, such as zombie PCs or illegally accessed servers to send spam e-mails. In this regard, ir is not just important, but necessary, to seek other types of regulatory remedies. For example, industry and government might coregulate mobile advertising, so that a government agency and an industry organization implement sorne sort of advance approval scheme together. The preapproval of mobile advertising messages by a coregulator with adjudicatory power might effectively reduce misleading or deceptive advertising, while the government monitors self-regulation and makes occasional recommendations.

Mobile users' privacy concerns are imperative for mobile advertisers. They worry about unfair information practices, but they also expect voluntary control from the industry. Government regulation requires privacy complaints to pass through a legal process, which tends to be lengthy and bureaucratic. Most mobile users therefore would prefer to avoid this venue if possible. Excessive legal control of information exchanges would make the use of time-space flexible mobile devices counterproductive. If mobile users believe that industry self-regulation is ineffective in preventing unfair information practices, however, they may cancel their implicit social contracts and seek remedy through governmentallegislation.

Limitations and Further Studies

Sorne theoretical and methodological limitations should be acknowledged with regard to these findings. First, although the general consumer sample employed in this srudy increases the externa! validity and generalizability of the results, the sample comes from a professional research firm's online panel, which may not be representative of the population of mobile phone users inJapan in all aspects. Second, despite the strong case for using Japan as the setting of this study, we must take into account its cultural, social, economic, and technological conditions when interpreting the results of this study. For example,Japanese consumers may have a very different concept of trust in the government than do people from the United States. Third, we use a three-point, single measure of the degree of regulatory control. However, because we do not ask respondents about their perceptions of the quickness, flexibility, and effectiveness of various regulatory options, these measures may not be able to capture users' true preferences.

Researchers should continue to investigare other attributes of consumer privacy concerns in mobile advertising. Of particular interese are the potencial additional moderators of the relationships among information privacy concerns, perceived risk, and preference for the degree of regulatory control, such as high versus low volumes of mobile ads, as perceived by users; opt-in versus opt-out effects; and large versus small compensation. Further insights could come from comparisons of the formation of information privacy concerns related to tradicional PC or "wired" advertising and those pertaining to mobile advertising. Finally, more theories should attempt to explain the dimensions of perceived ubiquity and its impact on mobile adverrising. Breakthrough research in mobile advertising regulation will require the deployment of multidisciplinary frameworks and methodologies, which remain a challenge for mobile technology researchers.

NOTE

l. The paths from perceived ubiquity to time flexibility and spatial flexibility are all statistically significant at $p < .001$, with standardized coefficients of .92 and .92, respectively.

REFERENCES

Bagozzi, Richard P., and Youjae Yi (1988), "On Evaluarían of Structural Equations Models," *Journal of the Academy of Marketing Science,* 16 (1), 74-94.

Barnes, Stuart J., and Sid L. Huff (2003), "Rising Sun: i-mode and the Wireless Internet," *Communications of the ACM,* 46 (11), 79-84.

Bart, Yakov, Shankar Venkatesh, Sultan Fareena, and L. Urban Glen (200'5), "Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study," *Journal of Marketing,* 69 (October), 133.

Barwise, Patrick, and Colín Strong (2002), "Permission-Based Mobile Advertising," *Journal of lnteractive Marketing,* 16 (1), 14-24.

Business Monitor Internacional *(2008),japan Telecommunications Report Q3 2008,* London.

Camerer, Colín F. (2003), "Psychology and Economics: Enhanced: Strategizing in the Brain," *Science,* 300 (5626), 1673-167'5.

Chen,Jengchung V., William Ross, and Shaoyu F. Huang (2008), "Privacy, Trust, and Justice Considerations for Location-Based Mobile Telecommunication Services," *Info,* 10 (4), 30-4'5.

Chin, Wynne W. (1998), "The Parcial Least Squares Approach for Structural Equation Modeling," in *Modern Methods for Business Research,* George A. Marcoulides, ed., Hillsdale, NJ: Lawrence Erlbaum, 29'5-336.

---,Barbara L. Marcolin, and Peter R. Newsted (2003), "A Partial Least Squares Latent Variable Modeling Approach for Measuring lnteraction Effects: Results from a Monte Carla Simulation Srudy and an Electronic-Mail Emotion/ Adoption Study," *Information Systems Research,* 14(2), 189-217.

Cho, Chang-Hoan, and Hongsik John Cheon (2004), "Why Do People Avoid Advertising on the Internet?" *Journal of Advertising,* 33 (4), 89-97.

Cloudmark (2008), "Mobile Operators Brace for Global Surge in Mobile Messaging Abuse" (February 11), available at www .marketwire.com/mw/rel_us_print.jsp?id=819426 (accessed March 28, 2008).

CNET.co.uk (2006), "Mobile Spam Spells Trouble for Text-Based Ads" (November 16), available at http://news.enet.eo.uk/ mobiles/0,39029678,49285278,00.htm (accessed April 4, 2008).

Corbin, Kenneth (2008), "Will Mobile Ads Finally Get Their Due?" *Internet News* (May 7), available at www.internetnews .com/mobility/article.php/3745286 (accessed August 12, 2008).

Diamantopoulos, Adamantios, and Heidi M. Winklhofer (2001), "Index Construction with Formative Indicarors: An Alternative to Scale Development," *journa! of Marketing Research,* 38 (May), 269-277.

Dinev, Tamara, and Paul Hart (2004), "Internet Privacy Concerns and Their Antecedents: Measurement Validity and a Regression Model," *Behaviour and Information Techno!ogy,* 23 (6), 413-422.

Dou, Xue, and Hairong Li (2008), "Creative Use ofQR Codes in Consumer Communication," *1nternational J ournal of Mobile Marketing,* 3 (2), 61-67.

Falk, R. Frank, and Nancy B. Miller (1992), *A Primer for Soft Modeling,* Akron, OH: University of Akron Press.

Fuller, Mark A., Mark A. Serva, andJohn Skip Benamati (2007), "Seeing Is Believing: The Transirory Influence ofReputation Information on E-Commerce Trust and Decision Making," *Decision Sciences,* 38 (4), 675.

Golembiewski, Roberr T., and Mark McConkie (1975), "The Centrality of Interpersonal Trust in Group Processes," in *Theories of Group Processes,* Cary L. Cooper, ed., New York: Wiley, 131-185.

Gupta, Anil K., and J. Lad Lawrence (1983), "Industry Self-Regulation: An Economic, Organizational, and Political Analysis," *Academy of Management Review,* 8 (3), 416-425.

Hagerstrand, Torsten (1975), "Space, Time and Human Conditions," in *Dynamic Allocation ofUrban Space,* A. Karlqvist, L. Lundquist, and F. Snickars, eds., Farnborough, UK: Saxon House, 3-14.

Hair, Joseph F., William C. Black, Barry J. Babin, Rolph E. Anderson, and Ronald L. Tatham (2006), *Multivariate Data Analysis,* Upper Saddle River, NJ: Prentice Hall.

Hawkins, Delbert L., Roger J. Best, and Kenneth A. Caney (2001), *Consumer Behavior: Building Marketing Strategy,* 8th ed., New York: McGraw-Hill.

Hulland, John S. (1999), "Use of Partial Least Square (PLS) in Strategic Management Research: A Review ofFour Recent Studies," *Strategic Managementjournal,* 20 (2), 195-204.

Jarvenpaa, Sirkka L., Noam Tractinsky, and Lauri Saarinen (1999), "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *]ournal of Computer-Mediated Communication,* 5 (2), available at www.ascusc.org/jcms/vO 15/issue2/jarvenpaa .html (accessed June 2, 2008).

Macneil, Jan R. (1974), "The Many Furures ofContracts," *Southern California Law Review,* 47 (3), 691-816.

---(1980), *The New Social Contract,* New Haven: Yale University Press.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Constructs, the Scale, anda Causal Model," *Information Systems Research,* 15 (4), 336-355.

Mathwick, Charla, Naresh Malhotra, and Edward Rigdon (200 1), "The Effecr ofDynamic Retail Experiences on Experiential Perceptions ofValue: An Internet and Catalog Comparison," *Journa! ofRetai!ing,* 78 (1), 51-60.

Mayer, Roger, James Davis, and F. David Schoorman (1995), "An lntegrative Model of Organizational Trust," *Academy of Management Review,* 20 (July), 709-734.

Metzger, Miriam J. (2004), "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication,* 9 (4), available at http:// jcmc.indiana.edu/vO 19/issue4/metzger.html (accessed September 11, 2008).

Milberg, Sandra J. H., Jeff Smith, and Sandra J. Burke (2000), "Information Privacy: Corporate Management and National Regulation," *Organization Science,* 11 (1), 35-57.

Milne, George R., and Mary Ellen Gordon (1994), "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contraer *Framework,"journal ofPublic Policy and Marketing,* 12 (2), 206-215.

Ministry of Interna! Affairs and Communications (2007), *White Paper: Information and Communications in Japan,* Information and Communication Statistics Database-Year 2005, Tokyo: Government of Japan (in Japanese).

---(2008), "Policies Related to Annoying Emails Prevention," available at www.soumu.go.jp/joho_tsusin/d_syohi/m_mail .html (accessed March 1, 2008) (in Japanese).

Miyazaki, Anthony D., and Ana Fernandez (2000), "Internet Privacy and Security: An Examination of Online Retailer *Disclosures,"]ournal ofPublic Policy and Marketing,* 19 (1), 54-61.

Mobile Marketing Association (2008), "Consumer Best Practices Guidelines" (July 9), available at www.mmaglobal.com/ bestpractices. pdf (accessed August 21, 2008).

Moorman, Christine, Rohit Deshpandé, and Gerald Zaltman (1993), "Facrors Affecting Trust in Market Research Relationships,"]ournal *of Marketing,* 57 (January), 81-101.

Nikkei Sangyo Shinbun (Nikkei industrial journal) (2006), "Combar Spam Mail" (February 24), 3 (inJapanese).

Nunnally, Jum C. (1978), *Psychometric Method,* New York: McGraw-Hill.

Okazaki, Shintaro, and Charles R. Taylor (2008), "What Is SMS Adverrising and Why Do Multinationals Adopt lt? Answers from an Empirical Study in European Markets," *Journa! of Business Research,* 61 (1), 4-12.

———, Akihiro Katsukura, and Mamoru Nishiyama (2007), "How Mobile Advertising Works: The Role of Trust in Improving Attitudes and Recall," *Journal of Advertising Research,* 47 (2), 165-178.

Pavlou, Paul A. (2003), "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *lnternational]ournal of Electroníc Commerce,* 7 (3), 101-134.

Petty, Ross D. (2003), "Wireless Advertising Messaging: Legal Analysis and Public Policy Issues," *Journal of Public Policy and Marketing,* 22 (1), 71-82.

Reedy, Sarah (2008), "Privacy and The Holy Grail ofMobility," *Telephony,* 249 (3), 24-27.

Rettie, Ruth, Ursula Grandcolas, and Bethan Deakins (2005), "Text Message Advertising: Response Rates and Branding Effects," *]ournal of Targeting, Measurement and Analysis for Marketing,* 13 (4), 304-312.

Rifon, Nora]., Robert LaRose, and Sejung Marina Choi (2005), "Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal *Disclosures,"]ournal ofConsumer Affairs,* 39 (2), 339.

Ringle, Christian M., Sven Wende, and Alexander Will (2005), *SmartPLS2.0(M3) Beta,* Hamburg: Universitat Hamburg, available at www.smartpls.de (accessed March 2, 2008).

Rose, Ellen A. (2006), "An Examination of the Concern for Information Privacy in the New Zealand Regulatory Context," *Information and Management,* 43 (3), 322-335.

Rotter,Julian B. (1971), "Generalized Expectancies for Interpersonal Trust," *American Psychologist,* 26, 443-452.

Schlosser, Ann E., Tiffany Barnett White, and Susan Lloyd (2006), "Converting Website Visirors into Buyers: How Website Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions," *Journal of Marketing,* 70 (April), 133-148.

Schoenbachler, Denise D., and Geoffrey L. Gordon (2002), "Trust and Customer Willingness ro Provide Information in Database-Driven Relationship Marketing," *]ournal of Interactive Marketing,* 16(3), 2-16.

Sheehan, Kim Bartel, and Maria G. Hoy (1999), "Flaming, Complaining, Abstaining: How Online Users Respond ro Privacy *Concerns,"journal of Advertising,* 28 (3), 37-51.

———, and (2000), "Dimensions of Privacy Concern Among Online Consumers," *]ournal of Public Policy and Marketing,* 19 (1), 62-73.

Smith, H.Jeff, SandraJ. Milberg, and SandraJ. Burke (1996), "Information Privacy: Measuring, Individuals' Concerns About Organizational Practices," *MIS Quarterly,* 20 (2), 167-196.

Stewart, Katherine J. (2003), "Trust Transfer on the World Wide Web," *Organization Science,* 14(1), 5.

Stewart, Kathy A., and Albert H. Segars (2002), "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research,* 13 (1), 36-49.

Sutherland, Ewan (2007), "The Regulation of the Quality of Service in Mobile Networks," *info,* 9 (6), 17-34.

Trend Micro (2001), "Virus and Malicious Code Protection for Wireless Devices," *Trend Micro White Paper* (February), available at www.digipoint.be/pdf/Trend/wireless.pdf (accessed March 2, 2008).

Tsang, Melody M., Shu-Chun Ho, and Ting-Peng Liang (2004), "Consumer Attitudes Toward Mobile Advertising: An Empirical Study," *International]ournal ofEiectronicCommerce,* 8 (3), 65-78.

Webster,Jane, and Linda K. Trevino (1995), "Rational and Social Theories as Complementary Explanations of Communication Media Choices: Two Policy-Capturing Studies," *Academy of Management]ournal,* 38 (6), 1544-1572.

Westin, Alan F. (1967), *Privacy and Freedom,* New York: Atheneum.

APPENDIX

Questionnaire Items

Information Request Scenarios

- *More sensitive information request:* Imagine that you have received an e-mail newsletter in your mobile phone to which you are subscribing from a mobile online shop. The newsletter lists an ad that invites you to entera sweepstake for its promotional campaign. The winning prize is an electronic coupon for music download, which will be received by a return e-mail in your mobile phone. The company requires you to key in your name, address, and household income as prerequisite for participation.
- *Less sensitive information request:* Imagine that you have received an e-mail newsletter in your mobile phone to which you are subscribing from a mobile online shop. The newsletter lists an ad that invites you to enter a sweepstake for its promotional campaign. The winning prize is an electronic coupon for music download, which will be received by a return e-mail in your mobile phone. The company requires you to key in your gender, age, and postal code.

Prior Negative Experience (Adapted from Cho and Cheon 2004)

1. I have seen my personal information misused by companies without my authorization.*
2. 1feel dissatisfied with my earlier choice to send my personal information to mobile advertisers.
3. My experience in responding to mobile advertising is very unsatisfactory.
4. In the past, my decision to send my personal information to mobile advertisers has not been a wise one.

Perceived Ubiquity

- *Timeflexibi!ity (adapted from Mathwick, Ma!hotra, and Rigdon 2001)*
  1. Using mobile Internet is an efficient way to manage my time.
  2. Browsing mobile Internet sites makes my life easier.*
  3. Browsing mobile Internet sites fits with my schedule.
- *Spatial flexibility-original items*
  1. Using mobile Internet enables meto find information at any place.
  2. Browsing mobile Internet gives mean ability to overcome spatiallimitations.
  3. Browsing mobile Internet sites fits any location, wherever I go.

Mobile Users' Information Privacy Concerns (Adapted from Malhotra, Kim, and Agarwal2004)

- *Collection*
  1. Itusually bothers me when mobile advertisers ask me for personal information.
  2. When mobile advertisers ask me for personal information, I sometimes think twice before providing it.
  3. It bothers meto give personal information toso many mobile advertisers.
  4. I'm concerned that mobile advertisers are collecting too much personal information about me.
- *Control*
  1. Consumer privacy in mobile devices is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
  2. Consumer control of personal information lies at the heart of consumer privacy.
  3. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
- *Awareness*
  1. Companies seeking information in mobile advertising should disclose the way the data are collected, processed, and used.
  2. A good consumer privacy policy in mobile advertising should have clear and conspicuous disclosure.

3. Iris very important tome that I am aware of and knowledgeable about how my personal information will be used by mobile advertisers.

Perceived Risk (Adapted from Malhotra, Kim, and Agarwal 2004)

1. In general, it would be risky to give (the information) ro online companies.
2. There would be high potential for loss associated with giving (the information) to online firms.
3. There would be too much uncertainty associated with giving (the information) ro online firms.
4. Providing online firms with (the information) would involve many unexpected problems.
5. I would feel safe giving (the information) ro online companies (reverse).*

Trust (Adapted from Schlosser, White, and Lloyd 2006)

- *Ability*
  1. Mobile advertisers seem very capable of performing mobile communications.
  2. Mobile advertisers appear to be successful at the things they try to do.
  3. Mobile advertisers seem to have much knowledge about what needs to be done to fulfill online communication.
  4. I feel very confident about mobile advertisers' online skills.
  5. Mobile advertisers appear to have specialized capabilities that can increase their performance with online communication.
- *Benevolence*
  1. Mobile advertisers seem very concerned about my welfare.*
  2. My needs and desires appear to be important to mobile advertisers.
  3. It doesn't seem that mobile advertisers would knowingly do anything annoying to hurt me.
  4. Mobile adverrisers seem ro really look out for what is important tome.
  5. Mobile advertisers appear ro go out of their way to help me.
- *Integrity*
  1. Mobile advertisers seem to have a strong sense of justice.
  2. Mobile advertisers appear to try hard to be fair in dealing with others.
  3. Mobile advertisers' actions and behaviors are not very consistent (reverse).*
  4. I like mobile advertisers' values.
  5. Sound principies seem to guide mobile advertisers' behavior.

Preference for the Degree of Regulatory Control-Original Items

I think information privacy in mobile advertising can be best protected and controlled by:

1. I don't know/cannot answer.
2. Industry self-regulations.
3. Coregulation.
4. Governmental regulations.

* Eliminated during the purification process of the measurement model assessment.