J. of the Acad. Mark. Sci. (2007) 35:572–585
DOI 10.1007/s11747-006-0003-3

ORIGINAL EMPIRICAL RESEARCH

Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective

May Lwin · Jochen Wirtz · Jerome D. Williams

Received: 24 August 2006 / Accepted: 28 August 2006 / Published online: 8 February 2007

Abstract We use the Power–Responsibility Equilibrium (PRE) framework and advance that consumers balance perceived deficits in privacy protection by power holders (businesses and regulators) with defensive actions. In our model, consumer privacy concern is the endogenous mediating entity linking business policy and regulatory perceptions to negative online user responses. The model was empirically tested and confirmed in an experimental setting. In a second study, we added the nature of consumer information involved into a sub-model. Here, we investigated the moderating role of information sensitivity and congruency on the business policy–concern relationship across three industry contexts. Both hypothesized two-way interactions were confirmed, suggesting that a strong business policy is effective in reducing concern when low sensitivity data are gathered, but insufficient in reducing concern for highly sensitive data. Furthermore, concern increased dramatically when sensitive data were collected that were incongruent with the business context.

M. Lwin
Division of Public and Promotional Communication,
School of Communication and Information,
Nanyang Technological University, 31 Nanyang Link,
SCI Bldg, 637718 Singapore, Singapore
e-mail: tmaylwin@ntu.edu.sg

J. Wirtz
NUS Business School, National University of Singapore,
1 Business Link, 117592 Singapore, Singapore
e-mail: jochen@nus.edu.sg

J. D. Williams (✉)
Department of Advertising, University of Texas at Austin,
1 University Station A1200, Austin, TX 78712-1092, USA
e-mail: jerome.williams@mail.utexas.edu

Keywords Online privacy · Power responsibility · Business policy · Regulation · Congruency-sensitivity interaction

Introduction

The same technological advances that have made the Internet a potent marketing tool have also multiplied the threats to user privacy. Information is being collected not just on those who register and shop, but also on those who use credit cards, e-mail (Caudill & Murphy, 2000), and even on those who merely surf. Many users take countermeasures to protect their privacy, including supplying false or fictitious information to a Web site (Lwin & Williams, 2003), managing the use of cookies (Culnan & Bies, 2003), and even refusing to purchase from particular Web sites (Culnan & Milne, 2001). Marketers need to address online consumer privacy concerns as they can undermine a firm's marketing effectiveness, especially given the shift of marketing transactions to the Internet (Gauzente & Ranchhod, 2001).

From a policy perspective, governments in many countries have recently given more consideration to consumer privacy policy in their efforts to regulate the Internet (Westin, 2003). In addition, heightened security needs since the terrorist attacks in 2001 have created tension between balancing civil liberties and stronger government surveillance, placing privacy high on the political agenda (Szynal, 2002).

In this paper, we seek to advance our understanding on how consumer actions are influenced by corporate policy and governmental regulations at the macro level by applying the Power–Responsibility Equilibrium (PRE)

framework. At the business level, we investigate how the nature of information firms collect influences the business policy–concern relationship.

Model development

The privacy literature can be organized into two broad streams. The first involves consumer-level research like the measurement of Internet privacy concerns (Sheehan & Hoy, 2000), and the examination of the specific conditions under which individuals would be willing to provide personal information (e.g., Moon, 2000; Phelps, Nowak & Ferrell, 2000). The second stream has concentrated on the ethical, legal, regulatory and public policy factors, and corporate responsibilities concerning online privacy (e.g., Bloom, Milne & Adler, 1994; Caudill & Murphy, 2000; Culnan, 2000). Our research links these two perspectives into an integrated framework using the PRE framework.

The PRE framework applied to Internet privacy

The PRE model, which originated from power relationship studies in sociology and social psychology (Emerson, 1962), holds that social power and social responsibility should go hand in hand (Murphy, Laczniak, Bowie, & Klein, 2005). The more powerful partner in a relationship has the societal obligation to ensure an environment of trust and confidence. According to the model, if a company chooses a strategy of greater domination and less responsibility, the company will lose in the long run as consumers take defensive actions to reduce the firm's power. This framework has been applied to business interactions, such as those between organizations and their members (Shenkar & Ellis, 1995), and between the franchisor and franchisee (Vlosky, Wilson, & Vlosky, 1997), but has not yet been applied to study the relationship between firms and their customers.

We propose that the partners in this exchange context are the corporations and government on the one side (i.e., the powerholders who should show responsibility), and the individual consumer on the other side who expects responsible use of power. Privacy concern, rather than being modeled as a dependent variable to policy, or an independent variable to response behaviors as in extant research, is modeled as a mediating variable between policy, regulation and response behaviors. As concern can play both causal and consequential roles, positioning it as an intermediary allows for an integrated systems view. It shows how the responsibility demonstrated by power-holders can act as a predictor of potentially damaging customer responses. Figure 1 summarizes our hypothesized model.

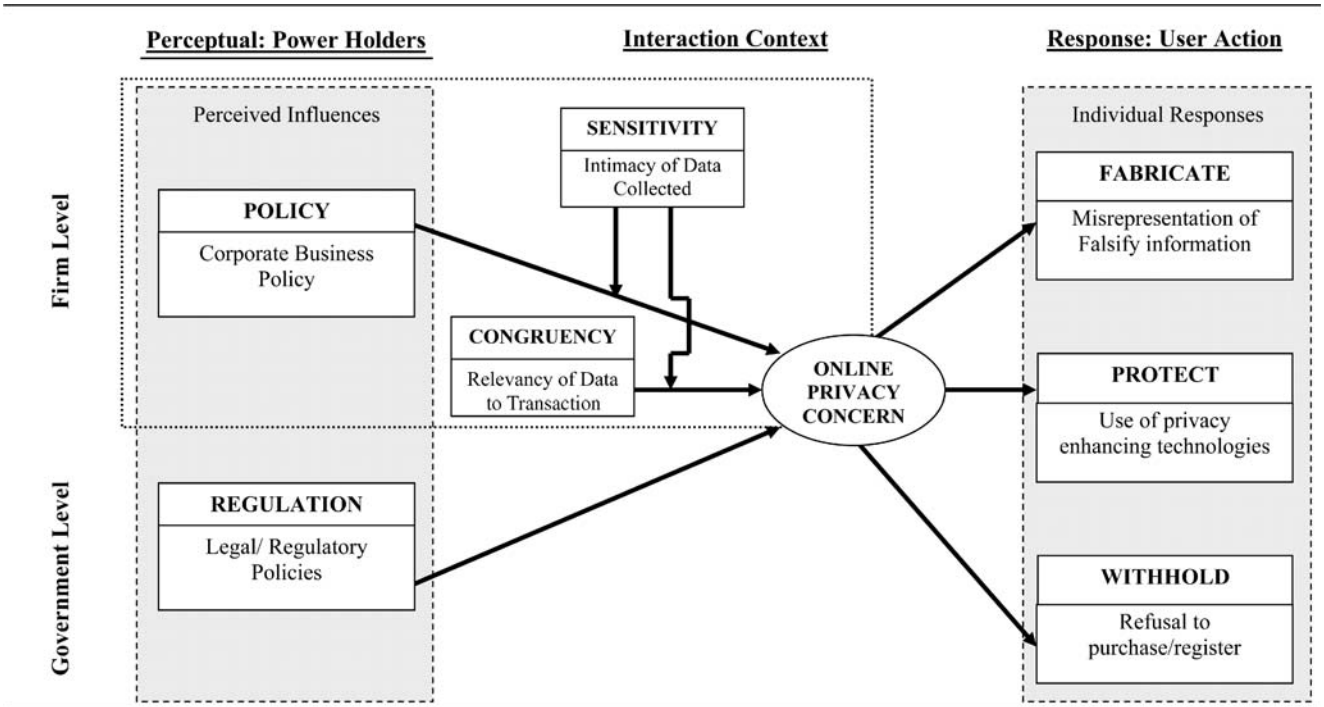

Figure 1 Conceptual model linking policy, regulation and context to user responses via a power–responsibility perspective.

Corporate policy, government regulation and privacy concern

Policy is the company policy as perceived by consumers of how a firm exercises ownership and power over the use of consumer data. Especially large organizations have inherent ethical responsibilities based purely on their size and power, and thus should be expected to show social responsibility (Murphy et al., 2005). While almost all U.S. Web sites state some kind of privacy policy, actual corporate policy pertaining to the level of privacy protection varies widely.

The link between perceived levels or quality of privacy policies on consumer privacy concern has received scant empirical attention (Caudill & Murphy, 2000). In the Internet context, many corporate privacy policies do not fully comply with Federal Trade Commission (FTC) guidelines, which in turn has been linked to heightened consumer privacy concerns (Culnan, 2000). Furthermore, half of those surveyed rarely or never read privacy notices (Culnan & Milne, 2001). However, the possibility of business practices regarding personal data being primarily responsible for people's privacy concerns has not been empirically tested. We propose that consumers' privacy concerns and subsequent actions are affected by consumer perceptions of corporate policies and practices.

Regulation refers to the perceived regulatory policies of how various government agencies, the other key power holders, devise Internet privacy regulation, and direct and police the use of consumer data. The state is generally seen as having the responsibility to ensure the well-being of consumers in cases of power imbalance (Goldring, 1990), and data protection concerns within the populace would generally be due to a perceived lack of regulation (Smith, 1994). For example, higher levels of privacy concern were found to be associated with more moderate regulatory environments (Milberg, Burke, Smith, & Kallman, 1995).

Internet users often have limited knowledge and resources to assess data security, and thus rely on institutional safeguards and laws to protect their civil rights. Regulation is seen as essential in protecting online privacy (Rust, Kannan, & Peng, 2002). We propose that perceived effectiveness of regulatory policies and their enforcement will reduce consumer online privacy concerns.

Consumer responses to privacy concern

Concern relates to the customers' apprehension and uneasiness over the use of their personal data (Robbin, 2001; Westin, 2003). We propose that online privacy concern mediates the effects of Policy and Regulation on user behavior. Specifically, we suggest that consumers' sense of how power-yielding parties exercise their responsibility towards privacy will have an impact on customer privacy concern and ultimately on their resultant defensive responses. These responses are what Emerson (1962) would call "balancing operations," and are the consequence of a perceived imbalance in the power–dependence relationship. For example, if an Internet user perceives that corporations are acting responsibly in terms of their privacy policies, and that sufficient legal regulations are in place and enforced to protect their privacy, users are expected to show less concern for Internet privacy and therefore not to resort to balancing operations. On the other hand, if those in power positions are not perceived as acting responsibly, consumer concern is likely to intensify, leading to defensive measures.

Defensive measures include responses at the immediate individual level as well as activities which comprise the consumer plus one or more third parties such as in complaining and lobbying. In this research, we focus on the three most frequently used individual defensive measures, namely the fabrication of personal information (*Fabricate*), adoption of protective measures (*Protect*), and refusal to transact with a Web site (*Withhold*). These responses are consistent with a variety of personal responses documented in previous studies on consequences of privacy and security concerns in marketing (e.g., Culnan & Milne, 2001; Phelps et al., 2000).

Fabricate means that consumers disguise their identity through the use of fictitious or false information (Lwin & Williams, 2003). Over 30% of Internet users admitted to routinely giving false or fictitious information to Web sites (Culnan & Milne, 2001), while more than half (51%) reported that they falsify or misrepresent data at least occasionally (Fox et al., 2000). Fabrication has been described as a "guerilla tactic" which individuals have resorted to in order defend their privacy (Fox et al., 2000). The likelihood of such behavior is higher when privacy concerns are high, and when there are significant benefits for registering with a Web site (Lwin & Williams, 2003).

Protect refers to the use of tools and technology to safeguard one's online privacy. They include anonymizers, encryption technologies such as Pretty Good Privacy (PGP), anti-spam filters, re-mailers, e-mail shredders, cookie-busters, and HTML filters. One in 20 users had employed software to hide their computer's identity from Web sites (Fox et al., 2000), while one in four had set their browsers to reject cookies (Culnan & Milne, 2001). We propose that with rising concern, consumers are more likely to use protection technologies.

Finally, *Withhold* means that a consumer refuses to provide information to a Web site or even to patronize it. Individual have been shown to abstain from participating in activities that might lead to privacy concerns (e.g., Culnan

& Milne, 2001; Phelps et al., 2000). We propose that consumers are more likely to withhold information in situations of high concern.

In sum, we propose that when concerned individuals are faced with a perceived power-responsibility imbalance, they will resort to counteractive behaviors to reduce the perceived lack of equilibrium. The following hypotheses summarize our discussion:

H1: Privacy concern mediates the causal relationship between perceived company privacy policy and protective consumer responses. Specifically, the weaker (less effective) the perceived company policy is, the higher will be the degree of privacy concern, and as a result, the higher will be the likelihood of users engaging in protective response behaviors, including degree of (a) fabrication of personal information, (b) adoption of protection technologies, and (c) withholding from interacting with a Web site.

H2: Privacy concern mediates the causal relationship between perceived online privacy government regulation and protective consumer responses. Specifically, the weaker (less effective) the perceived government online privacy regulation is, the higher will be the degree of privacy concern, and as a result, the higher will be the likelihood of users engaging in protective response behaviors, including degree of (a) fabrication of personal information, (b) adoption of protection technologies, and (c) withholding from interacting with a Web site.

Extending the base model

H1 and 2 were designed to test the overall integrated model. Next, in H3 and 4, we focus on the corporate-user interface and introduce contextual factors to the exchange. Although a number of contextual factors have been studied, such as the potential benefits of disclosure (Lwin & Williams, 2003), and privacy seals (Miyazaki & Krishnamurthy, 2002), the effect of the nature of data collected on privacy concern remains relatively unexplored. We focused here on the sensitivity of information to the customer and its perceived congruency to the interaction context. Both are important and managerially relevant dimensions of data privacy concerns, but have not yet been empirically studied.

Information sensitivity

Both theoretical and anecdotal evidence suggests an important role of data sensitivity (which is defined as the perceived intimacy level of information) in information privacy (e.g., Margulis, 2003; Westin, 2003). In surveys, a large percentage of respondents refused to give information they deemed as too personal or sensitive to a Web site (e.g., Culnan & Milne, 2001). We propose that our policy main effect on privacy concern is moderated by sensitivity. Specifically, policy should be highly effective in reducing concern for less sensitive data. However, as sensitivity increases, policy alone will become less effective in reducing concern, which will remain high when data are highly sensitive. Past research noted that while consumers generally feel comfortable providing e-mail addresses, most respondents would feel less comfortable providing their phone number (Cranor, Reagle, & Ackerman, 1999) and health data like medical records (Kam & Chismar, 2006). For highly sensitive information, such as income or health information, a comprehensive policy might be necessary but not quite sufficient to bring concern levels down to a low level, whereas for data with low sensitivity, a good policy might be sufficient.

H3: The hypothesized causal link in H1 from perceived company policy to privacy concern is moderated by the sensitivity of data being collected. Specifically, at low levels of sensitivity, a comprehensive privacy policy will reduce concern by a large margin, whereas at increasing sensitivity, the magnitude in concern reduction will decrease.

Information congruency

Congruency in marketing research refers to the level of interconnectedness of two stimuli. We define information congruency in the data collection context as the relevance of information being collected to the transaction context. For instance, privacy concern has been shown to be affected by the perceived congruency of data requested with the type of business. Specifically, when the data requested were congruent with the retail context (e.g., the information might be needed by the provider to customize service and communications), privacy concerns were reduced (Graeff & Harmon, 2002). This implies that a consumer would be less concerned when divulging one's grocery purchase information to a supermarket Web site as compared to an unrelated online business.

We propose that the strength of the congruency effect on concern is likely to be dependent on the sensitivity of information requested. For example, consumers may be generally comfortable providing insensitive information like their general interests (Robbin, 2001), while more sensitive information, such as one's salary or credit card details, is more likely to be viewed within a transaction context. As such, we expect congruency to have a stronger effect on concern when information of high rather than low sensitivity is involved. Following this line of argument, we propose in H4 that the impact of congruity on concern is moderated by data sensitivity.

H4: At high levels of data sensitivity, incongruency will lead to high levels of concern, whereas at decreasing sensitivity, the effect of incongruency on concern will decline.

Research method

To test our hypotheses, we conducted two controlled experiments using Web-based data collection. As we are concerned with Internet user behavior, using the e-platform seemed appropriate for our research context.

Measures

Table 1 provides an overview of our measures. They were all based on seven-point Likert-type scales in tandem with what was asked (for example, '1'=Not at All Concerned, and '7'=Extremely Concerned for *Concern,* and '1'=Very Unlikely, and '7'=Very Likely for *Protect*).

Perception of corporate business policy This measure was adapted from Smith, Milberg and Burke's (1996) scale of consumer opinions regarding organizational privacy practices. Three scale items were selected based on Karson's (2002) work, who adapted this scale to the Internet context to measure consumer perceptions of a company's online privacy policies and practices.

Perception of legal/regulatory policy No existing scales were found in the literature to measure the perception of legal and regulatory policy in the online privacy context. We therefore built on measures used in non-online privacy regulation research (e.g., Bennett, 1992; Milberg et al., 1995) to develop three statements for our context.

Online privacy concern A four-item scale was used. Two scale items were adapted from a study on Internet user attitudes about online privacy (Cranor, Reagle, & Ackerman, 1999). A further item was adapted from Milne and Boza's (1999) research on privacy concerns pertaining to database

Table 1 Measurement items

Construct	Measurement items	Cronbach alpha study	
		1	2
Policy	The company would not use personal information of consumers for purposes other than those initially stated at the site. (PO1)	0.83[a]	0.95[a]
	The company would not share your personal information with other external parties unless it has been authorized by individuals who provided the information. (PO2)		
	The company's databases that contain personal information are protected from unauthorized access regardless of costs. (PO3)		
Regulation	The existing laws in my country are sufficient to protect consumers' online privacy. (R1)	0.83[a]	N.A.
	There are stringent international laws to protect personal information of individuals on the Internet. (R2)		
	The government is doing enough to ensure that consumers are protected against online privacy violations. (R3)		
Concern	How concerned are you that your personal data may be used for purposes other than the reason you provided the information for. (C1)	0.86	0.95
	How concerned are you about your online personal privacy on this Web site? (C2)		
	How concerned are you about the fact that this Web site might know/track the sites you visited? (C3)		
	How concerned are you about this Web site sharing your personal information with other parties? (C4)		
Fabricate	I would consider making up fictitious responses to avoid giving the Web site real information about myself. (F1)	0.81	0.90
	I would resort to using another name or Web/e-mail address when registering with this Web site so I can have full access and benefits as a registered user without divulging my real identity. (F2)		
	When registering with this Web site, I would only fill up data partially. (F3)		
Protect	I would like to make use of software so that the recipient cannot track the origin of my mail (e.g., re-mailers). (P1)	0.72	0.92
	I would use software to eliminate Cookies that track my Web-browsing behavior (e.g., JunkBuster, WRQ AtGuard). (P2)		
	I would like to make use of software to disguise my identity (e.g., Zero Knowledge, Anonymizer, Freedom) (P3)		
Withhold	I would be reluctant to register with this Web site. (W1)	0.89	0.92
	I would refuse to provide personal information to this Web site. (W2)		
	I would avoid visiting this Web site. (W3)		

[a] This scale was used as a manipulation check.
N.A. Not applicable as this scale was not included in Study 2.

marketing. The final item was taken from a study on situation-specific dimensions of privacy concern (Sheehan & Hoy, 2000).

Fabricate It was operationalized as the likelihood of a respondent falsifying or misrepresenting personal information in an online context. Our three-item scale was adapted from measures of the 10th WWW Survey (Georgia Tech Research Corporation, 1998) and from an online fabrication behavior scale (Fox et al., 2000).

Protect We conducted a survey of 30 Internet users to identify commonly used privacy-enhancing tools or technology. Three groups of technologies emerged (encryption, Cookie-busters, and anti-tracking software), which we used to develop a three-item scale. Respondents were asked to rate the likelihood of use of these tools.

Withhold Withholding behavior was operationalized as the extent to which respondents would shy away from interacting with a Web entity because of privacy concerns. Our three-item scale was adapted from Sheehan and Hoy (1999).

All measures were extensively pretested, which resulted in minor amendments in the wordings of some questions and dropping of one item. In the final pre-test with 205 undergraduates, an exploratory factor analysis was conducted to confirm the unidimensionality of our constructs, with all items having factor loadings above 0.50.

Demographics

We used panels of adult respondents provided by a commercial research firm. All respondents had been Internet users. The overall demographic profile for the samples of our studies showed only slight variations. For both, most of the respondents were male (51.7 and 62.3% for Studies 1 and 2, respectively), between 18 and 39 years old (71.6 and 68.8%), and had at least high school education (96.6 and 99.2%). The majority of the respondents resided in the US (81.7 and 73.3%), with the remainder of the respondents mostly coming from internet-savvy nations (e.g., Canada and E.U. countries).

Study 1: testing the base model

The perceived effectiveness of business policy and governmental regulations were manipulated in a 3×3 between-subjects factorial design. A scenario method was used where we presented respondents with vignettes which contained our manipulations (Wirtz & Bateson, 1999). The three levels for the corporate policy manipulation were based on previous work, which had identified principles of sound privacy policy for Web sites (e.g., McGraw, 1999). For example, the low level Policy scenario asked respondents to consider a situation where they visited a Web site that did not display a Fair Information Practices notice, whereas the high level scenario involved a Web site with a comprehensive and highly visible Fair Information Practices notice (Culnan & Bies, 2003). Similarly, the low level Regulation manipulation asked respondents to assume interaction with a Web site hosted in a country with very little privacy regulation, and the high level scenario involved a Web site being hosted in a country with highly comprehensive privacy regulations (Milberg et al., 1995).

Research procedure

After extensive pre-testing of our manipulations and a pilot test, 180 subjects participated in the actual survey (20 in each treatment condition). Nine vignettes, one for each experimental condition, were posted at different websites. Subjects received an invitation email that contained the link to one of the experimental conditions. These solicitation e-mails were then sent to groups of randomly generated e-mail addresses provided by a commercial research firm. Each respondent who submitted a completed survey received five dollars as a monetary incentive via the commercial provider's incentive payment scheme.

Preliminary analysis and manipulation checks

The manipulation checks for Business Policy and Regulation were administered after measuring the dependent variables to avoid potential demand effects. Two-way ANOVA results revealed that the manipulations were successful. Specifically, the anticipated main effects were significant for Policy [$F(2,177)=428.7$, $p<0.001$] and for Regulation [$F(2,177)=439.6$, $p<0.001$] on their respective manipulation checks. The means were in the expected direction for Policy (1.80, 3.80, and 5.79) and Regulation (1.75, 3.87, and 5.65) for the low, medium, and high conditions, respectively. None of the other main or interaction effects reached significance, suggesting clean manipulations.

Testing hypotheses 1 and 2

We used Baron and Kenny's (1986) three sub-model approach of testing for mediation effects. In sub-model 1, a two-way ANOVA was performed to examine the effects of Policy and Regulation on Concern. We found significant main effects for Policy [$F(2,171)=9.6$, $p<0.001$] and for Regulation [$F(2,171)=14.1$, $p<0.001$]. The Policy by

Regulation interaction effect was insignificant [$F(4,171)=1.4$, $p=0.25$). All cell means were in the expected direction (see Table 2). Specifically, higher Policy resulted in lower Concern, and as the level of Regulation increased, Concern was reduced. These findings satisfy the first test for mediation showing that Policy and Regulation had a direct impact on our mediating variable Concern.

Sub-model 2 used Policy and Regulation as two independent factors, and instead of Concern, it used the three power-enhancing consumer responses as dependent variables. As expected, the Policy and Regulation multivariate main effect and all the univariate effects on our three dependent variables were significant (see Table 2). None of the interaction effects reached significance. As expected, the cell means for each of the power-enhancing responses decreased with increasing levels of Policy and Regulation. These findings fulfill the second condition for mediation and show that our independent variables had a significant impact on the dependent variables.

In sub-model 3, we introduced Concern as a covariate into the MANOVA of sub-model 2. As expected, the effects of Concern on Fabricate, Protect and Withhold were all highly significant (Table 2). The Policy multi- and univariate main effects became insignificant with the introduction of Concern into the model ($p>0.05$), indicating full mediation. In contrast, the Regulation multivariate and univariate main effects remained significant. This finding suggests that not all effects of Regulation on the response behaviors were mediated by Concern. An examination of the eta square values for Regulation showed a large drop from between 0.13 to 0.15 in sub-model 2 to 0.03 to 0.04 in sub-model 3. This finding suggests that in spite of the remaining significant effects of Regulation, response behaviors were largely mediated by concern.

In conclusion, the findings from the three sub-models suggest that Policy and Regulation significantly affect Concern (sub-model 1), as well as Fabricate, Protect and Withhold (sub-model 2). Concern fully mediated the relationship from Policy to the three response behaviors, and largely mediated the relationship from Regulation to the responses (sub-model 3). These results provide support for H1 and 2.

Study 2—information sensitivity and congruency

Manipulations and stimuli pre-testing

Study 2 used a 2×3×2 (Policy × Sensitivity × Congruency) between-subject factorial design across three different industries (banking, car rental, and medical service). Using three services allowed us to examine the robustness of our findings across industry contexts and operationalizations of data lists for the sensitivity and congruency manipulations.

Table 2 Study 1: MANOVA results on power-balancing behaviors

Sub-model 2—Testing of direct effects								
Dependent variables	Multivariate		Univariate results					
	Results		Fabricate		Protect		Withhold	
	F	Sig.	*F*	Sig.	*F*	Sig.	*F*	Sig.
Policy (*P*)	3.7	0.001	7.2	<0.001	4.6	<0.001	10.0	<0.001
Regulation (*R*)	6.8	<0.001	14.1	<0.001	13.3	<0.001	15.3	<0.001
P×*R*	1.5	>0.10	1.5	>0.10	1.70	>0.10	1.8	>0.10
Sub-model 3—Inclusion of concern as a covariate								
Concern	43.0	<0.001	80.1	<0.001	94.5	<0.001	63.2	<0.001
Policy (*P*)	1.5	>0.10	1.2	>0.10	1.4	>0.10	2.9	>0.05
Regulation (*R*)	2.4	0.03	3.9	0.02	4.0	0.02	4.8	0.01
P×R	1.3	>0.10	1.0	>0.10	1.1	>0.10	1.2	>0.10
Manipulations	Cell means							
		Concern	Fabricate	Protect	Withhold			
Policy	Low	6.02	6.12	5.77	6.13			
	Medium	5.62	5.83	5.71	5.71			
	High	5.30	5.48	5.33	5.31			
Regulation	Low	6.02	6.26	6.03	6.21			
	Medium	5.75	5.81	5.54	5.74			
	High	5.16	5.37	5.23	5.20			

Subjects were randomly directed via an e-mail with a link to one of 36 different Web sites, each of which contained one of the experimental conditions (i.e., 12 cells across three industry contexts). For example, a particular scenario described an online bank with a highly impressive privacy policy (policy manipulation) asking respondents to disclose highly sensitive financial information (sensitivity manipulation) that is congruent with the industry context such as credit card number, home phone number, bank account details and income (congruency manipulation).

Policy was manipulated in the same manner as in Study 1. Specifically, in the low policy condition respondents were asked to assume visiting a fictitious Web site where there was no mention of a privacy policy. In the high policy condition, a comprehensive privacy policy was provided. Sensitivity and Congruency were manipulated by requesting a battery of five data items from each respondent. In the low sensitivity condition, respondents were asked for low sensitive information, and in the high sensitivity condition for mostly highly sensitive information. To develop effective sensitivity and congruency manipulations we performed a number of pre-tests. We first generated a detailed list of commonly solicited data items on financial, car rental and medical services Web sites. The inventory of data items ranged from name, phone number, and marital status, to income, occupation, medical history and most frequently used car rental company. In our first pre-test, we asked 24 students to rate the sensitivity of each data item (independent of industry), and the congruency of the data item with each of the three industries on a seven-point scale. This pre-test was used to classify common data items into groups of high, medium and low sensitivity, and high and low congruency for each of the three industries (see Table 3 for the sensitivity and congruency ratings of the items selected for our final manipulations).

The second pre-test was qualitative in nature. We conducted in-depth face-to-face discussions with ten respondents on which combination of data items should be selected from each of the low, medium, and high categories in our manipulations. These discussions resulted in a combination of five items for each of the six cells per industry (see Table 3). Care was taken to combine items that together were seen as credible and realistic, while at the same time resulting in the respective experimental conditions. Also, we maintained the same items across the three industries as far as possible without compromising realism in our scenarios. For example, the same data point could be coded as congruent in one context but incongruent in another (e.g., congruency scores for medical history was rated 5.92 out of 7 in the medical service context, but only 2.08 in the banking context).

In addition to the five items used to manipulate the experimental conditions, our pre-tests showed that respondents expected certain items to be present when Web sites ask for information. To enhance the realism of our manipulations, we therefore added name and e-mail address as two dummy items at the beginning of each of our five-item data batteries. A third pre-test with 30 students confirmed that the six experimental conditions (i.e., the three sensitivity and two congruency manipulations) were perceived as intended across three industries. That is, five-item batteries plus the two dummy items were tested across 18 cells (i.e., six cells across three industry contexts, see Table 3).

Research procedure

Solicitation e-mails were sent to groups of randomly generated e-mail addresses provided by the commercial directory service provider. We offered five Amazon.com vouchers ranging from $20 to $100 as lucky draw incentives for respondents who replied within 4 weeks. Reminder e-mails followed after 2 weeks. We received a total of 627 responses, of which 205 were for the bank scenario, 192 for the car rental, and 230 for the medical services scenario.

Manipulation checks

Manipulation checks were administered after the measures for our dependent variable to avoid potential demand effects. The Policy manipulation check was identical to that used in Study 1. The Sensitivity and Congruency manipulation checks consisted of two questions each. For Sensitivity, subjects were first asked a direct question on information sensitivity: “Would you consider the information being asked by this Web site sensitive?”(anchored in ‘1’=not very sensitive, and ‘7’=very sensitive). How personal a piece of data is seen is one aspect of information sensitivity (Margulis, 2003). Therefore, the following second question was asked: “How personal is the information being requested?” (anchored in ‘1’=not at all personal, and ‘7’=extremely personal). For Congruency, subjects were asked, “Would you consider the information asked by the Web site relevant to the company?” (anchored in ‘1’= not relevant at all, and ‘7’=very relevant), and “Did you expect the Web site to ask you for this set of information?” (anchored in ‘1’=not expected at all, and ‘7’=very much expected).

We conducted three four-way ANOVAs with the policy, sensitivity and congruency manipulations as well as the industry context as independent variables on each of the three manipulation checks. The results showed the intended main effects. Specifically, the main effects were significant on their respective manipulation checks for *Policy* [$F(1,625)=2,433.1$, $p<0.001$], *Sensitivity* [$F(2,624)=500.7$,

Table 3 Pre-test cell means for the sensitivity and congruency manipulations

	Low sensitivity			Medium sensitivity			High sensitivity		
	Banking	Car rental	Medical service	Banking	Car rental	Medical service	Banking	Car rental	Medical service
High congruency	Age (2.42; 5.17)	Age (2.42; 5.17)	Age (2.42; 6.00)	Employ. Status (3.83; 5.71)	Employ. Status (3.83; 4.02)	Employ. Status (3.83; 6.42)	Social Security no. (6.67; 5.63)	Mobile/pager no. (6.42; 5.17)	Social security no. (6.67; 5.21)
	Lang. preferred (2.17; 4.52)	Lang. preferred (2.17; 4.83)	Lang. preferred (2.17; 4.33)	Home address (5.92; 5.58)	Home address (5.92; 5.92)	Home address (5.92; 5.71)	Credit card no. (6.42; 4.21)	Credit card no. (6.42; 5.50)	Past med. test rslts. (4.92; 6.17)
	Marital status (2.63; 5.58)	Car Rental co. (1.92; 5.04)	Marital status (2.63; 5.42)	Employer info (4.33; 4.21)	Employer info (4.33; 5.36)	Medical insurance (4.12; 5.36)	Home phone no. (6.38; 4.03)	Home phone no. (6.38; 5.58)	Medical history (4.71; 5.92)
	Residing country (1.92; 4.33)	Travel habits (2.88; 4.00)	Residing country (1.92; 4.33)	Occupation (2.25; 3.57)	Auto insurance (4.00; 5.25)	Health condition (4.50; 5.92)	Bank acct. details (6.13; 4.92)	Home addres (5.92; 5.92)	Home addres (5.92; 5.71)
	General interest (1.79; 4.45)	Gender (2.33,3.88)	Gender (2.33,4.92)	Mortgage info (3.92; 4.58)	Car accident hist. (3.96; 4.83)	Ethnic group (4.21; 4.46)	Income (5.00; 4.33)	Date of birth (5.08; 4.50)	Date of birth (5.08; 5.58)
Cell means pre-test 3	2.00; 5.60	2.00; 5.80	2.20; 5.60	3.60; 5.40	4.00; 6.00	4.00; 5.80	5.40; 5.40	6.00; 5.80	5.60; 5.60
Low congruency	Reading habits (2.13; 2.25)	Reading habits (2.13; 2.63)	Reading habits (2.13; 2.08)	Health condition (4.50; 2.29)	Health condition (4.50; 2.88)	Car accident hist. (3.96; 2.83)	Homepage URL (5.04; 2.88)	Homepage URL (5.04; 2.29)	Homepage URL (5.04; 2.83)
	Mobile operator (2.13; 2.33)	Mobile operator (2.13; 2.54)	Mobile operator (2.13; 2.17)	Car accident hist. (3.96; 2.25)	Yrs. work exp. (3.92; 2.63)	Yrs. work exp. (3.92; 2.29)	Date of birth (5.08; 3.21)	Bank acct. details (6.13; 2.50)	Bank acct. details (6.13; 2.25)
	General interest (1.79; 2.13)	Employ. sector (2.42; 2.13)	Employ. sector (2.42; 2.73)	Ethnic group (4.21; 1.92)	Ethnic group (4.21; 1.79)	Auto insurance (4.00; 2.71)	Religion (5.21; 2.13)	Religion (5.21; 1.79)	Credit card details (5.92; 2.13)
	Travel habits (2.88; 2.29)	Web knowledge (1.92; 2.83)	Web knowledge (1.92; 2.58)	Auto insurance (4.00; 2.58)	Mortgage info (3.92; 2.76)	Mortgage info (3.92; 2.23)	Past med. test rslts. (4.92; 2.17)	Source of income (5.08; 2.46)	Source of income (5.08; 2.79)
	Car rental co. (1.92; 2.17)	General interest (1.79; 2.13)	Car rental co. (1.92; 1.79)	Medical insurance (4.12; 2.27)	Highest edu. lvl. (3.08; 2.25)	Highest edu. lvl. (3.08; 2.13)	Medical history (4.71; 2.08)	Medical history (4.71; 2.42)	Income (5.00; 2.53)
Cell means pre-test 3	2.00; 2.00	2.00; 1.80	1.80; 2.40	3.80; 2.80	3.60, 2.40	3.80; 2.00	6.00; 1.80	5.80; 2.40	5.40; 2.40

The first number in each cell refers to the Sensitivity and the second to the Congruency mean score for the individual data items obtained in Pre-test 1, and the mean scores for the 18 (9×2) overall 5-item batteries were obtained from Pre-test 3.

Table 4 Study 2: summary ANOVA results

Group	Main effects			Interaction effects			
	Policy (*P*)	Congruency (*C*)	Sensitivity (*S*)	*S*P*	*S*C*	*C*P*	*S*C*P*
Banking	*F*=56.6**	*F*=36.2**	*F*=21.2**	*F*=8.5**	*F*=9.6**	*F*=1.5	*F*=0.1
Car rental	*F*=17.4**	*F*=25.6**	*F*=11.5**	*F*=2.5a	*F*=5.9**	*F*=0.7	*F*=0.1
Medical service	*F*=46.0**	*F*=16.6**	*F*=24.3**	*F*=10.9**	*F*=4.5*	*F*=1.0	*F*=0.8

**$p<0.01$, *$p<0.05$, [a] $p=08$

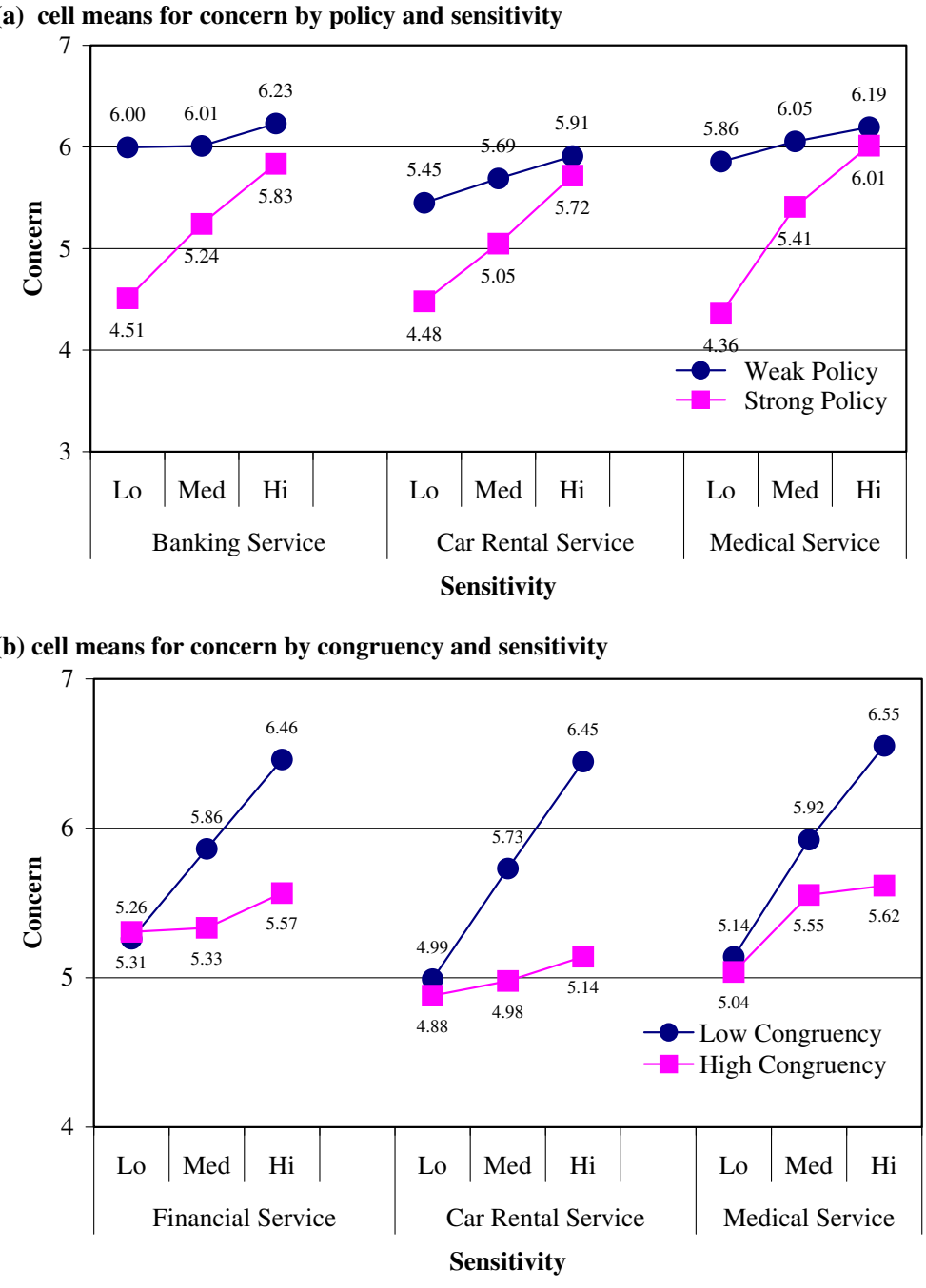

Figure 2 Study 2: interaction effects on concern.

Table 5 Study 2: cell means for concern by policy, sensitivity, and congruency conditions

		Banking			Car rental service			Medical service		
		Sensitivity			Sensitivity			Sensitivity		
		Low	Med	High	Low	Med	High	Low	Med	High
Policy	Weak	6.00	6.01	6.23	5.45	5.69	5.91	5.86	6.05	6.19
	Strong	4.51	5.24	5.83	4.48	5.05	5.72	4.36	5.41	6.01
	Delta	1.49	0.77	0.40	0.97	0.64	0.19	1.50	0.64	0.18
	t-value	5.97**	2.80**	1.89	3.60**	2.19*	0.80	7.19**	2.86**	0.96
Congruence	Low	5.26	5.86	6.46	4.99	5.73	6.45	5.14	5.92	6.55
	High	5.31	5.33	5.57	4.88	4.98	5.14	5.04	5.55	5.62
	Delta	−0.05	0.53	0.89	0.11	0.75	1.31	0.10	0.37	0.93
	t-value	−0.15	1.83	4.66**	0.35	2.63**	7.39**	0.37	1.58	5.95**

**$p<0.01$, *$p<0.05$

$p<0.001$], and *Congruency* [$F(2,625)=278.7$, $p<0.001$]. All cell means were in the expected direction. They were 2.17 and 5.69 for weak and strong Policy, 2.79, 4.55, and 5.66 for low, medium and high Sensitivity, and 3.19 and 4.68 for low and high Congruency. Also, none of the interaction effects nor the industry main effect reached significance ($p>0.10$). Together, these results indicate that our manipulations were successful.

Testing hypotheses 3 and 4

The data were analyzed using three-way ANOVAs, one for each industry context, to examine the hypothesized moderating effect of Sensitivity on the Policy–Concern relationships (H3), and the Sensitivity moderation effect on the congruency–concern relationship (H4).

The main effects of Policy and Congruency on Concern were significant across all three industry contexts (see Table 4). Consistent with H3 and 4, we found two significant two-way interaction effects. First, the interaction between Sensitivity and Policy was highly significant for banking and medical services, and marginally significant for car rental ($p=0.08$). The cell means in Fig. 2a and Table 5 show that concern could be significantly reduced with a strong policy in the low and medium data sensitivity conditions across all three industry contexts (e.g., for banking, low data sensitivity: $\overline{X}_{\text{weak policy}} = 6.00$ vs. $\overline{X}_{\text{strong policy}} = 4.51$, $t=5.97$, $p<0.01$, and for medium sensitivity: $\overline{X}_{\text{weak policy}} = 6.01$ vs. $\overline{X}_{\text{strong policy}} = 5.24$, $t=2.80$, $p<0.01$; see Table 5). However, in the high sensitivity condition, concern remained high even with a good privacy policy (e.g., for banking,: $\overline{X}_{\text{weak policy}} = 6.23$vs.$\overline{X}_{\text{strong policy}} = 5.83$, $t=1.89$; $p>0.05$), confirming H3. It may be that a good privacy policy is a necessary but not sufficient condition for concern to be reduced when highly sensitive data is involved.

Second, the interaction between Sensitivity and Congruency was significant for all three contexts (see Table 4). The cell means for the Congruency-Sensitivity interaction on Concern are in the direction as advanced in H4 (Fig. 2b). Information congruency had a strong and significant effect on concern in the high information-sensitive condition across all three industries (e.g., for banking: $\overline{X}_{\text{low congruency}} = 6.46$vs. $\overline{X}_{\text{high congruency}} = 5.57$, $t=4.66$; $p<0.01$; Table 5). Conversely, the effect became insignificant in the low sensitivity condition (e.g., for banking: $\overline{X}_{\text{low congruency}} = 5.26$ vs. $\overline{X}_{\text{high congruency}} = 5.31$, $t=0.15$; $p>0.10$), supporting H4. These findings suggest that congruency is important when highly sensitive data are involved. Here, concern increases dramatically if the requested information is incongruent with the business context.

Discussion and implications

Summary findings and theoretical implications

Our findings support the applicability of the PRE model, a comprehensive, theory-based framework, as a foundation for incorporating new ideas regarding antecedents and consequences (e.g., the use of protection technologies) to privacy concern. The framework is unique in that it allows for an integrative view of separate spheres in the privacy literature. First, consumer–business and citizen–government relationships in the context of privacy research have been largely disconnected (Westin, 2003), which the PRE framework integrates. Second, in the marketing literature, concern has either been modeled as a dependent variable to policy and other variables, or as a causal antecedent to various consumer behaviors. Our study positions concern both as a consequent variable as well as a mediating variable between these interdependent variables that again allows an integrated systems view (see Fig. 1). This positioning links existing research streams, for example, in examinations of corporate policies and practice versus

associating specific privacy concerns to user responses. The framework implies that larger corporations in particular should manage privacy in a responsible manner (or risk power loss) and could also be applied to other types of regulatory activity on the part of businesses and governments that have a bearing on the public, for example, in the regulation of advertising and promotions.

The results from Study 1 show that firms and regulators need to be perceived as acting responsibly in their utilization of personal data if they wish to avoid negative balancing actions by consumers. The findings support the hypotheses that the level of defensive responses is impacted by consumers' perceived notions as to how good corporate and governmental policies are in protecting consumer interests. We also demonstrated that privacy concern is a key mediating entity linking both business policy and regulatory perceptions to negative online user responses.

In Study 2, we focused on the business policy-side by including information sensitivity and congruency into a sub-model. Both are managerially highly relevant variables that have not been studied in a privacy context before. Here, we have two key findings. First, a robust business policy can play an important role in influencing concern when the information requested is low in sensitivity. However, even a comprehensive policy appears insufficient to alleviate concern when highly sensitive information is involved. Second, our information congruity–sensitivity interaction effect implies that congruency has a sizeable impact on highly sensitive data. Specifically, concern increased dramatically when the data requested were incongruent with the business context. Conversely, congruency seemed to matter little for less sensitive data. These findings were consistent across the three industry contexts studied.

Managerial implications

Our findings indicate that consumers look to both organizational policies and governmental regulations to safeguard their online privacy. Firms can enhance consumer's perception of their privacy protection by working within and outside their organizations to achieve a responsibility balance with end users. This is at odds with how many organizations deal with privacy issues at present, where often mainly external threats seem to act as catalysts for crafting and communicating cohesive policies and practices (Culnan & Bies, 2003). Correcting this reactive posture would involve proactively evaluating all collection procedures and usage of customer data, and the implementation, enforcement and external communication of a comprehensive privacy policy. Firms should work with industry bodies and regulators to develop mutually beneficial and practical plans for promoting privacy regulations within their industries, including promoting effective self-regulation and third-party accreditations. At a minimum, firms should ensure that their corporate policy on privacy is communicated via short but comprehensive privacy notices that are highly visible on their Web sites (Milne & Culnan, 2004).

The finding that the nature of information collected plays a key role in influencing concern is managerially interesting. Our policy–sensitivity interaction shows that although an excellent privacy policy can be effective in reducing privacy concern, it is insufficient when highly sensitive information is being collected. Furthermore, the congruency–sensitivity interaction on concern showed that congruency matters, especially for highly sensitive data. Highly sensitive information appears to create an over-arching consideration, whereby consumers consider whether the data collected is congruent to the firm's business. To reduce privacy concerns, the information requested should be perceived as congruent with the transaction context. To achieve this, businesses could explicitly communicate why information is needed and how it is relevant to its business, and how information disclosure would benefit the consumer (e.g., through more customized and convenient service; Graeff & Harmon, 2002).

Implications for public policy

Our findings suggest that policy makers need to manage perceptions of privacy regulation. Policy efforts to improve privacy protection should be clearly communicated to the public along with the creation of a response outlet for privacy concerns (Milne & Culnan, 2004). While legislators and academics are divided on whether there should be increased government intervention in the enforcement of more stringent data protection measures on businesses (Reidenberg, 1996), it is likely that consumers would have less concerns if they perceived that policy makers were arbitrating an effective legal framework for protecting privacy on the Internet (Hiller & Cohen, 2001). Within the U.S., positive developments include policy makers increasingly turning their attention to privacy legislation that attempts to lessen consumer privacy concern (e.g., California's Database Security Breach Notification Act at the state level, and The Health Insurance Portability and Accountability Act (HIPAA) at the federal level).

As perceived governmental regulation influences consumer responses, we agree with Hiller and Cohen (2001) that an overall information protection system to address privacy might be preferable over individual statues separately focusing on specific areas of potential misuse of information (e.g., The Right to Financial Privacy Act of 1978; HIPAA 1996). An overarching regulatory approach which covers all sectors and types of data collection is more likely to improve general user views on regulatory comprehensiveness, rather than a piecemeal approach.

Future research

Our study focused on the users' initial interaction with a Web site where concern was studied as a mediator influencing response behaviors. Other variables such as trust, risk and privacy orientation provide logical avenues for future research, especially in the CRM context when customers build experience with a Web entity and face potential future disclosure situations. For example, researchers have suggested that violation of trust through a breach of the firm's information practices may raise concerns and ambivalence about future disclosure (Culnan & Bies, 2003). In addition, as our study was cross-sectional, future work could investigate delayed consumer actions using longitudinal data. Also, future research could utilize other methods that include real time data from Web sites or data from laboratory experiments.

Finally, our findings also should hold relevance to non-Internet contexts where personal data are being collected. This would be the case in industries using CRM, loyalty or membership programs. It would be of interest to extend our work to contexts such as mail order, call-center delivered services, and even supermarket chains which use loyalty programs and the like to collect an enormous amount of detailed transaction data to improve the cost effectiveness of their marketing (e.g., ranging from communications, sales to cross-selling campaigns) and to improve their customer service (e.g., to prioritize, customize and personalize service delivery). Much interesting work lies ahead to understand privacy in increasingly complex environments.

References

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173–1182.

Bennett, C. J. (1992). *Regulating Privacy*. Ithaca, New York: Cornell University Press.

Bloom, P. N., Milne, G. R., & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal consideration. *Journal of Marketing, 58*(January), 98–110.

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing, 19*(Spring), 7–19.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). Beyond concern: Understanding net users' attitudes about online privacy. *AT&T Labs–Research Technical Report TR 99.4.3*.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*(Spring), 20–26.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59* (2), 323–342.

Culnan, M. J., & Milne, G. R. (2001). *The Culnan–Milne survey on consumers and online privacy notices*. (accessed August 8, 2006). [available at: http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf].

Emerson, R. M. (1962). Power-dependence relations. *American Sociological Review, 27*, 31–40.

Fox, S., Lee, R., Horrigan, J., Lenhart, A., Tom, S., & Carter, C. (2000). Trust and privacy online: Why Americans want to rewrite the rules.

Gauzente, C., & Ranchhod, A. 2001. Ethical marketing for competitive advantage on the internet. *Academy of Marketing Science Review* (Online). 01 (10).

Georgia Tech Research Corporation (1998). 10th WWW user survey, (accessed January 8, 2001), [available at: http://www.cc.gatech.edu/gvu/user_surveys].

Goldring, J. (1990). Common law and legal theory: Reflections of a common lawyer. *Journal of Consumer Policy, 13*(2), 113.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *The Journal of Consumer Marketing, 19*(4/5), 302.

Hiller, J. S., & Cohen, R. (2001). *Internet Law and Policy*. NJ: Prentice-Hall.

Kam, L. E., & Chismar, W. G. (2006). Self-disclosure: Model for the use of internet-based technologies in collecting sensitive health information. *International Journal of Healthcare Technology and Management, 7*(3/4), 5.

Karson, E. J. (2002). Exploring a valid and reliable scale of consumer privacy and security concerns on the internet and implications for e-commerce. *Paper presented at Academy of Marketing Science Conference*, May 29–June 2, Sanibel, FL.

Lwin, M. O., & Williams, J. D. (2003). A model interpreting the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters, 14*(4), 257–272.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*(2), 243–261.

McGraw, H. IIII. (1999). Managing the privacy revolution. *Direct Marketing*, 61 (April), 36–40.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information, privacy and regulatory approaches. *Communications of the ACM, 38*(12), 65–74.

Milne, G. R., & Boza, M. E. (1999). Consumers' trust and concern about organizations use of personal information in direct marketing. *Journal of Interactive Marketing, 13*(Winter), 7–24.

Milne, G. R., & Culnan, M. J. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read [or Don't Read] Online Privacy Notices. *Journal of Interactive Marketing, 18*(3).

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *The Journal of Consumer Affairs, 36*(1), 28–49.

Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers. *Journal of Consumer Research, 26* (March), 323–339.

Murphy, P., Laczniak, G. R., Bowie, N. E., & Klein, T. A. (2005). *Ethical marketing: Basic ethics in action*. Upper Saddle River, NJ: Prentice-Hall.

Phelps, J. E., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19*(Spring), 27–41.

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal, 45*.

Robbin, A. (2001). The loss of personal privacy and its consequences for social research. *Journal of Government Information, 28*(5), 493–527.

Rust, R., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of Academy of Marketing Science, 30* (4), 455–464.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How online users respond to privacy concerns. *Journal of Advertising*, 28 (Fall), 37–51.

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

Shenkar, O., & Ellis, S. (1995). Death of the organization man: Temporal relations in stategic alliances. *The International Executive, 37*(6), 537.

Smith, H. J. (1994). *Managing privacy: Information technology and corporate America*. Chapel Hill, N.C.: University of North Carolina Press.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20 (June), 167–196.

Szynal, D. (2002). Internet proposals await lawmakers. *Marketing News, 36* (Jan 7), 11.

The Health Insurance Portability and Accountability Act of 1996 (1996). Public Law 104-91, 104th Congress, August 21, 1996, accessed at http://aspe.hhs.gov/admnsimp/pl104191.htm. December 19, 2006.

The Right to Financial Privacy Act of 1978 (1978). Public Law 95-630, November 10, 1978, accessed at http://www.fdic.gov/regulations/laws/rules/6500-2550.html, December 19, 2006.

Vlosky, R. P., Wilson, D., & Vlosky, R. (1997). Closing the inter-organizational information systems relationship satisfaction gap. *Journal of Marketing Practice, 3*(2), 75.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431–453.

Wirtz, J., & Bateson, J. E. G. (1999). Consumer satisfaction with services: Integrating the environmental perspective in services marketing into the traditional disconfirmation paradigm. *Journal of Business Research, 44*(1), 55–66.