Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis

George R. Milne and Shalini Bahl

Despite previous examinations of business actions, consumer reactions, and regulatory efforts, there has been no direct comparison of consumer and marketer expectations for establishing and respecting privacy boundaries. This study directly compares consumer segments' and marketers' expectations for privacy boundaries that regulate marketers' access to consumers and their information. Using data from a national online survey, the authors compare three consumer segments' preferences regarding the boundaries for the use of eight information technologies (cookies, biometrics, loyalty cards, radio frequency identification, text messaging, pop-up advertisements, telemarketing, and spam) with survey results of marketing managers and database vendors for the same set of questions. The results identify consumer segments and technologies for which consumer expectations differ from marketers and, thus, for which more regulatory and public policy attention and research scholarship is needed.

Keywords: privacy, information technologies, consumer segmentation, opt-in/opt-out, managers versus consumers

The juxtaposed perspectives of marketers and consumers regarding proper use of information technologies for marketing have the potential to create conflicts over the protection of consumer privacy (Bloom, Milne, and Adler 1994). Throughout history, the introduction of new information technologies has created privacy concerns (Smith 2000); even today, marketers' use of technologies such as cameras, telephones, computer, the Internet, and now mobile technologies all raise questions about how information is captured and used. As new technologies are introduced and use becomes widespread, marketers and consumers must work out the norms of information capture and use.

The norms for information exchange between marketers and consumers have centered on what type of privacy boundary a consumer expects and permits (Culnan 1993; Milne 1997; Phelps, Nowak, and Ferrell 2000). Do consumers provide unrestricted access and disclosure? Do the levels of access and disclosure require the marketer to gain permission, or is permission restricted to allow no access? In addition to the role of consumer choice in setting boundaries, the norms for boundaries are set in part by legislative actions through privacy laws such as the Children's Online Privacy Protection Act (1998), the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (2003), and the Telephone Consumer Protection Act (1991). Trade association policies, such as the Direct Marketing Association's (2010) "Online Marketing Guidelines," have also been adopted to engender trust between marketers and consumers. The media has also acted as a watchdog, identifying issues that need addressing when imbalances between the expectations of marketers and those of consumers occur (Roznowski 2003). Finally, consumer behavior, in terms of adoption of the technologies, and complaint behavior regarding the improper use of technologies have helped shape the playing field between marketers and consumers (Peltier, Milne, and Phelps 2009).

As noted in the literature (Lwin, Wirtz, and Williams 2007; Regan 1995), it is important for public policy to assess the exchange relationship between marketers and consumers. To this end, ethical perspectives (Caudill and Murphy 2000; Sarathy and Robertson 2003), theories of power equilibrium (Lwin, Wirtz, and Williams 2007), and procedural justice (Ashworth and Free 2006; Culnan and Armstrong 1999) have proposed frameworks that suggest why marketers' actions affecting consumer privacy should be aligned with consumer expectations. In a self-regulating environment, congruency of expectations can lead to higher levels of trust and a more munificent environment for all. When expectations are being met by some firms and not by others, consumers can shift their business to firms that meet their expectations. However, if there is more widespread failure on behalf of firms to meet customer expectations, this serves as an indicator of where the self-regulatory envi-

George R. Milne is Associate Professor of Marketing, Isenberg School of Management, University of Massachusetts Amherst (e-mail: milne@mktg.umass.edu). *Shalini Bahl* is founder of iAM Business Consulting (e-mail: shalini@iam-bc.com). The authors thank the anonymous *JPP&M* reviewers for their valuable comments. George Franke served as associated editor for this article.

ISSN: 0743-9156 (print), 1547-7207 (electronic)

Journal of Public Policy & Marketing
Vol. 29 (1) Spring 2010, 138–149

ronment is breaking down and where corrective action through legislation or heightened self-regulatory action is needed.

Despite business actions, consumer reactions, and regulatory efforts, there has been no comparison of consumers' and marketers' expectations for establishing and respecting privacy boundaries. The extant empirical research has focused on either consumers or marketers. Indeed, there is a substantial literature on assessing consumer preferences for privacy boundaries (Bellman, Johnson, and Lohse 2001; Krishnamurthy 2001; Milne and Rohm 2000; Miyazaki and Fernandez 2001). There is also a growing literature that investigates marketer policies (Culnan 2000; Hoy and Phelps 2003; Milne and Culnan 2002; Miyazaki and Fernandez 2000; Sheehan 2005). The current study extends these research streams by comparing the preferences of consumers, overall and at the segment level, with those of marketers on the same set of scenarios and measures. Specifically, we compare the privacy boundary expectations of the different consumer segments with those of marketing managers and database marketing vendors for eight scenarios depicting the use of different information technologies. This research contributes to the marketing and policy literature by measuring norms of expectations and showing where there are gaps between marketers and consumers to guide additional regulatory attention.

We organize the remainder of this article as follows: We being with the conceptual background to frame the research questions. Then, we present the methodology, the results, and the public policy implications and offer some conclusions.

Conceptual Background

Privacy regulation theory describes the processes by which consumers and marketers maintain privacy boundaries that govern their interactions. Altman's (1975) seminal work on this theory views the privacy boundary as a dialectic process in which people change the opening and closing of boundaries over time depending on specific situations. A person tries to optimize the amount of privacy he or she desires; balance is achieved when actual privacy equals desired privacy. The boundary framework has also been used to examine dyadic information exchanges (Derlega and Chaikin 1977) and communication (Petronio 2002). This research stresses that boundary setting is a dialectic process that involves people in considering risks and benefits. It also notes that turbulence between exchange partners can occur when there is not an agreement on what the boundaries should be.

The current research is predicated on the following contextual specifications: First, the privacy boundaries regulating the information and interaction exchange between marketers and consumers can be viewed in terms of allow, opt-out, opt-in, and do-not-allow decisions (Krishnamurthy 2001; Milne and Rohm 2000). Second, both consumers and marketers consider the risks and benefits in setting their preferences for privacy rules (Milne and Boza 1998, 1999). Third, the choice of privacy rules can vary by consumer segment and type of marketers (Dolnicar and Jordaan 2007; Smith 1994). Fourth, the preference of privacy rules can vary across technologies and their level of regulation (Peltier, Milne, and Phelps 2009). Details of these contextual specifications follow.

Privacy Boundaries

Consumers have needs they must balance when creating privacy boundaries, and marketers have needs they consider when deciding whether to respect consumers' boundaries. Privacy regulation theory (Altman 1975; Derlega and Chaikin 1977) suggests that two interacting parties will attempt to set boundaries that meet their individual goals as well as their collective interest. When the parties' goals and boundary expectations differ, there is "boundary turbulence." In support of the notion of turbulence, previous empirical research in a traditional direct marketing context has suggested that consumers and marketers view exchange differently (Campbell 1997; Cespedes and Smith 1993; Milne and Boza 1998) and that marketers want more access to consumers than consumers are comfortable in providing.

Traditionally, direct marketers have used opt-out choice formats to gain permission to use consumer information and to contact them in the future. The advantage of the opt-out choice for marketers is that it includes consumers in a program unless they specifically take action to remove themselves from lists. Such a framing has the potential to provide marketers with more names than opt-in lists, which require prior permission (Bellman, Johnson, and Lohse 2001). Conversely, opt-in or permission marketing options are viewed as giving consumers more control and as a better approach for building trust (Kristhnamurthy 2001). With opt-in, marketers are required to obtain prior permission before using information or contacting consumers. The privacy boundary setting will also depend on the situational context. For new technologies or technologies that are particularly invasive, it is plausible that some consumers will not want to provide any access and/or that marketers will not expect any access. Other consumers may be less aware of the privacy implications of the new technologies but may become uncomfortable after they become informed. Conversely, for technologies that have been in use for a long time, both consumers and/or marketers may not consider permission necessary.

Consumers' Background

Research has shown that consumers have varying levels of privacy concerns (Dolnicar and Jordaan 2007; Kumaraguru and Cranor 2005; Milne and Gordon 1994). Consistent with this, the Harris Interactive Opinion Poll segments consumers according to a privacy sensitivity index (Kumaraguru and Cranor 2005). In the 2004 Harris Poll, three segments ranging from very concerned to unconcerned were identified: privacy fundamentalists, privacy pragmatists, and privacy unconcerned. The fundamentalists believed that people should refuse to give marketers information and favored stronger laws to control the actions of organizations. The privacy pragmatists weighed the value of providing information to organizations and preferred voluntary programs for consumer choice rather than regulation. The privacy unconcerned had little problem with supplying firms with information and did not perceive any value in regulation. These segments represented 26%, 64%, and 10% of the

U.S. adult population, respectively. In the academic literature, Milne and Gordon (1994) find that consumer segments vary in terms of the privacy trade-offs they are willing to make. In a study of the Australian and South African markets, Dolnicar and Jordaan (2007) suggest that by segmenting consumers by privacy concerns, marketers are better able to target these consumers without violating consumer privacy expectations. To date, research has not investigated the extent to which consumer segments' privacy expectations match up with those of marketers.

Marketers' Background

Company and industry background affects the level of institutional privacy assurance, which is the interventions that a company makes to protect consumer privacy (Xu et al. 2008). Smith (1994) conducted one of the first examinations of company privacy practices by qualitatively studying the different issues and privacy practices in the banking, insurance, and health fields. Other research has examined direct marketers' attitudes toward privacy and direct/database marketing practices (Campbell 1997; Milne and Boza 1998). Industries that are more information intensive are more prone to higher levels of concern and less trust by consumers. Milne and Boza (1999) find that consumers have lower levels of trust for and more concern about direct marketers than other industries. Consistent with these findings, throughout the last decade, the Direct Marketing Association (2009) has actively advocated activities countering consumers' concerns. Despite this background, the question remains whether marketers from different industries have different privacy boundary expectations?

Use and Regulation of Technologies

The use of information technologies, while beneficial to marketers, has caused concern among consumers and public policy makers because some marketers overstep the boundaries of acceptable practice (Holtzman 2006). Consumer privacy is violated when information is gathered or used without consumer consent or when a consumer's private space is violated by unwanted consumer communications (Goodwin 1991). In this article, we investigate eight technologies that have been controversial within the last decade (see Table 1).

As Table 1 shows, the technologies that we investigate have different levels of regulation in place and offer different boundary management mechanisms to consumers. Some technology applications, such as telemarketing, text messaging, and spam, have resulted in legislative response from the U.S. government (e.g., CAN-SPAM Act 2003; Federal Trade Commission [FTC] 2003, 2009a; Telephone Consumer Protection Act 1991) that has partially addressed some privacy concerns. Other practices, such as cookies, pop-up advertisements, and loyalty cards, are not regulated at the federal level. Covert use of cookies and pop-up advertisements continue to be of concern to consumers (McCoy et al. 2007; Miyazaki 2008). Cookie uses in conjunction with behavioral advertising have come under intense legislative scrutiny by the FTC (2007, 2009b), but no legislation has been passed to regulate marketers' use of cookies. Emerging applications of technologies such as radio frequency identification (RFID) tags and biometrics have raised the alarm of public interest organizations and scholars (Langenderfer and Linnoff 2005; Peslak 2005; Tsang, Ho, and Liang 2004), but consumers' level of knowledge of and concern about the same is yet to be established.

For all technologies, a central question that remains unaddressed is, What is the privacy boundary that consumers prefer? In addition, How and when are marketer privacy boundary expectations in line or not in line with consumer expectations?

Research Questions

Building on our framework and the preceding discussion, we address the following research questions in the empirical study:

RQ1: To what extent do consumers and marketers agree on whether privacy boundaries should be open, closed, or permission based across technologies?

RQ2: When permission is selected, to what extent do consumers and marketers agree on whether opt-in or opt-out formats are preferred?

RQ3: Are there differences in privacy preferences between general marketing managers and employees in the database marketing industry?

RQ4: To what extent do different consumer segments agree with marketing managers on whether privacy boundaries should be open, closed, or permission based across technologies?

RQ5: Across which technologies do consumer segments want more restrictive boundaries than marketing managers?

Method

Questionnaire

The survey data for this study are based on eight scenarios involving information technologies (see the Appendix). The use of scenarios in empirical research has been found to be effective in evaluating ethical market behavior (e.g., Smith and Cooper-Martin 1997) and in e-commerce research (Ackerman, Cranor, and Regale 1999). In the scenarios, we measure whether the respondent believed that the activity (1) should be allowed; (2) should be allowed unless people object (opt-out) by telephone, e-mail, or written notice; (3) should be allowed only if prior permission is given by telephone, e-mail, or written notice (opt-in); or (4) should not be allowed.

The scenarios were pretested extensively according to the procedures Hunt, Sparkman, and Wilcox (1982) outline. We began by showing the instrument to eight researchers who were experts in survey design. Some provided verbal protocols while filling out the survey; others provided detailed written comments. Next, we ran two pretests with 145 and 124 students from two major state universities. Students answered questions about their preferred control mechanism for each scenario and their familiarity with the technology. Students were familiar with most technologies except RFID tags. In some cases, students noted wording that was unclear. Changes to the scenarios were made after each stage of the pretest.

It is inherently difficult to make comparisons across scenarios given the differences in their perceived tone and in the benefits and risks attached to each technology.

Table 1. Comparison of Boundary Management Mechanisms for Information Technologies

Technology	Regulation	Boundary Management Mechanisms
Cookies	FTC held town hall meetings to address cookie use with respect to behavioral advertising November 2007 and made recommendations February 2009.	Current approaches for controlling cookies can be confusing (Dixon 2008). Consumers can opt in or opt out through individual privacy policies. Consumers can sign up for persistent cookies to remember their Web sites through an opt-in mechanism. It is possible for passwords managed through opt-in mechanisms. Finally, consumers can globally opt out by downloading opt-out cookies.
Biometrics	The European Union has plans to put biometric information in passports (Findbiometrics.com 2009).	Notice and opt-in have been recommended by privacy researchers (Langenderfer and Linnoff 2005). When some technologies are implemented, consumers might be forced to use biometrics.
Loyalty cards	California Civil Code 1749.60 prohibits supermarkets from selling personal identifying information to third parties (Bosworth 2005).	Consumers Against Supermarket Privacy Invasion and Numbering (2008) is concerned about unfair pricing and loss of privacy. Although most consumers can opt in to programs, there are some instances of automatically being entered into Web-based loyalty programs. It is also possible for consumers to opt out of specific programs, such as information sharing.
RFID	FTC workshop in 2005. Washington State made it a felony to skim information from RFID readers without permission (Burnell 2008).	Recommended to give notice and choice to deactivate chip at time of purchase (Peslak 2005). Opt-out is implied if the chip is left active after purchase (Kelly and Ericson 2005) and requires schemes that include having consumers go to a Web site to deactivate or use the privacy enhancing technologies that block or kill the chips. Opt-in, as considered by the European Unioin, would disable the chip at the time of purchase and then be turned on only if consumer requests it through the use of a password (O'Connor 2008).
Text messaging	There are two sets of federal regulations that are currently applied to text message advertising: the Telephone Consumer Protection Act (1991) and the CAN-SPAM Act (2003).	Providing phone number with marketing effort has opt-out option for future text contact. Research suggests that consumers are negative unless there is opt-in. Approaches for opt-in have been successful in Japan.
Pop-up advertisements	Laws such as Washington's Computer Spyware Act (2005) limit embedding spyware in pop-up advertisements (Cain 2008).	Pop-up blockers enable consumer to opt out globally. Blockers can be customized to allow opt-in on some Web sites. Controlling pop-up advertisements is now possible through the use of pop-up blocker software available in most browsers. Still, the issue of spyware being embedded in pop-up advertisements continues to be a problem and warrants further regulatory attention (Cain 2008).
Telemarketing	The Do Not Call legislation (FTC 2003), with more than 145 million telephone numbers registered as of February 2007, has been effective.	Do Not Call lists allow global opt-out. For existing relationships, consumers rely on individual company opt-in or opt-out procedures (FTC 2003).
Spam	The CAN-SPAM Act (2003), which was passed to counteract many of the unethical elements of unsolicited commercial e-mail. The act restricts advertising e-mail when there is no previous or existing business relationship.	The CAN-SPAM Act controls nonrelationship situations. The act bans false or leading header information, prohibits deceptive subject lines, requires that the e-mail gives recipients an opt-out method, and requires that commercial e-mail is identified as an advertisement (FTC 2009a). It is up to consumers to decide what business relationships they want to enter (through opt-in or opt-out mechanisms) and to remove themselves from future communications if they so desire.

Although a neutral balance of risk/benefit for each scenario was sought, it was not always attained. For example, the scenario for telemarketing can be perceived as risky (and negatively worded), while cookies, biometrics, and loyalty cards can be perceived as having more benefits (because of positive wording). The scenario for biometrics, which pertains to body measurements, is different from the fingerprint and eye-scanning biometric use that is of greatest concern. Because there was not always a balance between risk and benefits across scenarios, we restrict comparisons to the differences of consumer and manager groups that viewed the same scenario.

Measures

The measures consisted of the same eight scenarios and specific demographic questions appropriate for each of the survey audiences. For each scenario, i = 1, ..., 8, there was a four-point ordinal variable reflecting the level of control desired (1 = allow, 2 = opt-out, 3 = opt-in, 4 = do not allow). From this variable, we created binary measures (1 =

yes, 0 = no) that indicated whether the response category was selected for each technology i. Next, we created a binary measure called permission (1 = yes, 0 = no), indicating for each scenario whether an opt-out or opt-in category was selected. To measure overall propensities, summated measures are counts of how many times respondents chose each control alternative across the eight technologies. We calculated percentages of format choices made across the eight technologies for each respondent.

The reliabilities (coefficient alphas) for the summated variables were $T_{not\ allow}$ = .758, $T_{opt\text{-}in}$ = .667, $T_{opt\text{-}out}$ = .682, and T_{allow} = .705. We used these measures to create market segments.

For comparison of privacy boundary preferences, we examined three broad levels: open, closed, and permission based. The open level is based on the percentage of respondents who selected the allow option. The closed level is based on the percentage of respondents who selected the do-not-allow option. The permission-based level is based on the percentage of respondents who selected either opt-in or opt-out.

Surveys and Responses

Three surveys were conducted: a consumer online survey, a mail survey of marketing managers, and a drop-off survey with database marketing vendors. Harris Interactive administered the final consumer online survey. A stratified random sample of 2027 adults was drawn from the Harris Online panel so that it reflected the U.S. adult online population: 47.5% were men, their average age was 45 years, 30.8% were college graduates or postgraduates, 33.6% had household income greater than $75,000, and they spent an average of 18 hours per week online (excluding e-mail).

The second survey of marketing managers was constructed using the same eight scenarios developed for the consumer survey. At the top of the survey, the respondents were instructed to answer from their perspective as a marketer. A direct mail business list was purchased of 1600 people with the title of marketing manager who were randomly selected from across the United States. From this list, 171 names were unusable because the person was no longer with the company, resulting in a mailing of 1439 pieces. Two waves of surveys were mailed. For the first wave, a personalized survey was sent out with a signed cover letter; the second wave was a reminder letter and copy of the survey. In total, there were 162 usable responses, for a response rate of 11.2%: 52.4% worked in their industry for more than 10 years, 72.1% worked in companies with sales less than $50 million, 70.7% were older than age 35, and 69% had an active database on consumers. A listing of titles showed that the sample did not include direct marketers. A comparison of early and late responders on their demographic characteristics revealed no statistical differences.

A third survey was adapted for data collection from database marketing vendors. The same eight scenarios from prior research were used. They were administered to marketing exhibitors at a direct marketing tradeshow. A survey was dropped off with 150 vendors, resulting in 79 qualified responses, for a response rate of 52.7%. The survey instructed respondents to answer from the perspective of a database marketing vendor. Of the respondents, 34.2% worked in the direct marketing industry for more than 10 years, 51.9% worked for companies with less than $50 million annual sales, 51.9% had an active database on consumers, and 30.4% reported using consumer information more intensely than average companies in the industry.

Data Analysis

We identified differences between consumers and marketing managers, consumers and database vendors, and marketing managers and database vendors on their privacy boundary preferences through tests of proportions for independent populations. We calculated a z-test for the overall results and at the scenario level for each group comparison. The results of this analysis for differences in preferences for open, closed, and permission-based boundaries (including the percentage that was opt-in) appear in Table 2. Differences between consumer segments and marketing managers were also examined for open, closed, and permission-based boundaries (including the percentage that was opt-in) through tests of proportions shown in Table 3.

We segmented consumers on the basis of total propensities for choosing the not-allowed ($T_{not\ allow}$), opt-in ($T_{opt\text{-}in}$), opt-out ($T_{opt\text{-}out}$), and allow (T_{allow}) options. To help determine the number of clusters, we took a subsample of the

Table 2. Comparison of Consumer, Marketing Manager, and Database Vendor Privacy Boundary Expectations

	Percentage Choosing Privacy Boundary			Z-Tests of Proportions Between Groups		
	Consumers	Marketing Managers	Database Vendors	Consumers Versus Marketing Managers	Consumers Versus Database Vendors	Marketing Managers Versus Database Vendors
N	2027	162	77			
Open	6.9	7.9	19.6	–.48	–4.19**	–2.63**
Closed	45.5	25.3	14.1	4.98**	5.44**	1.96*
Permission	47.6	66.8	66.3	–4.70**	–3.22**	.08
% of permission choosing opt-in	72.5	59.7	45.1	2.79**	4.21**	1.73

*$p < .05$.
**$p < .01$.

Table 3. Comparison of Consumer Segments' and Marketing Managers' Privacy Boundary Expectations

	Percentage Choosing Privacy Boundary				Z-Tests of Proportions		
	Receptive Segment	Balanced Segment	Restricted Segment	Marketing Managers	Receptive Versus Marketing Managers	Balanced Versus Marketing Managers	Restricted Versus Marketing Managers
N	384	801	842	162			
Open	19.4	3.8	4.3	7.9	3.35**	–2.30*	–1.95
Closed	20.4	28.1	73.4	25.3	–1.27	.73	11.81**
Permission	60.2	68.1	22.3	66.8	–1.45	.32	–11.38**
% of permission choosing opt-in	35.2	87.8	74.2	59.7	–4.25**	7.13**	2.59**

*$p < .05$.
**$p < .01$.

data and ran a hierarchical cluster analysis. The scree plot of the clustering coefficients suggested a three-cluster solution. Next, we ran a k-means clustering algorithm and selected a three-group solution, which matches the three segments Westin articulates in his Harris policy polls (Kumaraguru and Cranor 2005). The segments were profiled according to age, hours per week online, percentage of male respondents, percentage of college graduates, and percentage of income greater than $75,000 (see Table 4). There were statistically significant differences in means of the profile variables (expect hours online) across the segments.

From the pattern of responses in Table 4, we named the first segment (N = 801, 40% of sample) the "balancers." The balancers were most likely to select the opt-in choice (4.79). Their demographics reflect the average profile. The second segment (42% of sample) was the "restricted" segment. As the name implies, they are most likely to select the not-allow choice (5.87). As with the balancers, they had very low incidences of opting out (.46) or allowing technologies (.30). The restricted segment was the youngest, was the least educated, and had the lowest income. The third and smallest segment (19% of sample) was the "receptive" segment. The receptive segment had the highest incidences for opting out (3.12) and allowing the technology (1.55). The receptive segment was the oldest, most likely to be male, most educated, and most affluent.

Results

RQ1: To what extent do consumers and marketers agree on whether privacy boundaries should be open, closed, or permission based across technologies?

A higher percentage of consumers preferred closed boundaries than marketing managers and database vendors. There were statistically significant differences between consumers and marketing managers (45.5% versus 25.3%; z = 4.98, $p < .01$) and between consumers and database vendors (45.5% versus 14.1%; z = 5.44, $p < .01$). Consistent with these results, a lower percentage of consumers want a permission-based boundary than marketing managers and database vendors. There were statistically significant results between consumers and marketing managers (47.6% versus 66.8%; z = –4.70, $p < .01$) and between consumers and database vendors (47.6% versus 66.3%; z = –3.22, $p < .01$).

Table 4. Segmentation Results

	Total	Balanced Segment	Restricted Segment	Receptive Segment	F	Probability (F)
N	2027	801	842	384		
Total not allowed	3.64	2.25	5.87	1.63	2196.4	.000
Total opt-in	2.76	4.79	1.32	1.70	1820.9	.000
Total opt-out	1.04	.66	.46	3.12	869.5	.000
Total allowed	.55	.30	.34	1.55	222.5	.000
Age	45.5	44.6	41.8	48.1	23.2	.000
Hours on Internet per week (not e-mail)	17.9	17.6	18.0	18.3	.296	.744
					χ^2	Probability (χ^2)
Male (%)	46.4	45.1	44.1	54.2	11.7	.003
College graduate (%)	47.0	48.6	42.7	53.1	11.4	.003
Income $75,000+ (%)	23.1	24.3	19.4	28.6	13.9	.001

*$p < .05$.
**$p < .01$.

With respect to open boundaries, there were no statistical differences between the percentage of consumers and marketing managers (6.9% versus 7.9%, n.s.). However, there were statistical differences between the percentage of consumers and database vendors who wanted open boundaries (6.9% versus 19.6%; z = –2.63, $p < .01$).

RQ2: When permission is selected, to what extent do consumers and marketers agree on whether opt-in or opt-out formats are preferred?

When respondents selected a permission-based boundary, a higher percentage of consumers (72.5%) than marketing managers (59.7%) and database vendors (45.1%) selected an opt-in format. The differences between consumers and marketing managers (z = 2.79, $p < .01$) and database vendors (z = 4.21, $p < .01$) were both statistically significant.

RQ3: Are there differences in privacy preferences between general marketing managers and employees in the database marketing industry?

Overall, a lower and statistically significant percentage of marketing managers than database vendors wanted open boundaries (7.9% versus 19.6%; z = –2.63, $p < .01$). In terms of the percentage who wanted permission-based boundaries, there were no overall statistically significant differences between marketing managers and database vendors (66.8% versus 66.3%; z = .08, $p > .05$). In terms of the percentage desiring closed boundaries, marketing managers had statistically significant higher levels than database vendors (25.3% versus 14.1%; z = 1.96, $p < .05$).

RQ4: To what extent do different consumer segments agree with marketing managers on whether privacy boundaries should be open, closed, or permission is needed across technologies?

The receptive segment had a higher propensity for open boundaries than marketing managers (19.4% versus 7.9%; z = 3.35, $p < .01$); there were no statistical differences for permission-based boundaries (60.2% versus 66.8%, n.s.) and closed boundaries (20.4% versus 25.3%, n.s.). In contrast, for the balanced segment, compared with marketing managers, there were no statistically significant differences for closed boundaries (28.1% versus 25.3%, n.s.) or permission-based boundaries (68.1% versus 66.8%, n.s.). However, although percentages were small, there was a statistically significant lower propensity for open boundaries (3.8% versus 7.9%; z = –2.30, $p < .05$). The restricted segment had a statistically higher propensity for closed boundaries than marketing managers (73.4% versus 25.3%; z = 11.81, $p < .01$), a statistically significant lower propensity for permission-based boundaries (22.3% versus 66.8%; z = –11.38, $p < .01$), and no differences for open boundaries (4.3% versus 7.9%, n.s.).

We further examined the extent to which consumer segments, compared with marketing managers, preferred the opt-in alternative. Comparing marketing manager opt-in propensities with those of the three consumer segments, we found varied differences. The receptive segment was less likely to choose opt-in when requesting permission than marketing managers (35.2% versus 59.7%; z = –4.25, $p < .01$). In contrast, the balanced segment was more likely to choose opt-in than marketing managers (87.8% versus 59.7%; z = 7.13, $p < .01$). Finally, the restricted segment was also more likely to choose opt-in than marketing managers (74.2% versus 59.7%; z = 2.59, $p < .01$).

RQ5: Across which technologies do consumer segments want more restrictive boundaries than marketing managers?

The analysis at the technology level in Table 5 shows proportions and statistical differences comparing the receptive, balanced, and restricted segments with marketing managers for each of the eight technologies. As the table shows, the restricted segment expected more protection than marketing managers for every technology (restricted > marketing managers, $p < .01$). For the restricted segment, the technologies that resulted in the largest differences for consumers wanting closed boundaries compared with marketers were cookies (80.6% versus 12.3%), e-mail (84.1% versus 24.7%), pop-up advertisements (91.1% versus 35.2%), and telemarketing (73.2% versus 19.1%). Compared with marketing managers, the balanced segment had a higher percentage who preferred closed boundaries for cookies (25.5% versus 12.3%; z = 3.63, $p < .01$) and pop-up advertisements (48.3% versus 35.2%; z = 3.05, $p < .01$). Compared with marketing managers, the receptive segment did not have a statistically higher percentage of the closed option for any technology.

Discussion

This study found differences in boundary expectations between marketers and consumers. Overall, consumers were more likely to choose closed boundaries than marketers, while marketing managers preferred to have most exchange interactions subject to permission-based boundaries. Few consumers or marketers reported that an open boundary setting would be best for these technologies. The overall differences between consumers were further highlighted by the finding that when permission-based boundaries were selected, a higher percentage of consumers than marketing managers wanted an opt-in choice. Although all marketers wanted fewer restrictions, there were differences among them; database vendor values were much less aligned with consumers than marketing managers. At first glance, it appears that in terms of the macroview and power frameworks, firms are not being responsive to consumers' needs.

However, there is a limitation of analyzing privacy issues at too high a level of aggregation and not focusing on the customer segment level (Dolnicar and Jordaan 2007). It has been suggested that by segmenting consumers according to their privacy concerns, it is possible to target them more effectively by taking into account privacy considerations (Dolnicar and Jordaan 2007). To address this, we segmented consumers into the three groups of receptive, balanced, and restricted segments, which were consistent with previous privacy segmentation schemes (Kumaraguru and Cranor 2005) that reflected low-, medium-, and high-concern groups. However, the current research differs in that we measured privacy boundary preferences, while Westin (see Kumaraguru and Cranor 2005) measured general privacy

Table 5. Comparison of Market Segment Boundary Preferences with Marketing Managers by Technology

	Percentage Choosing a Privacy Boundary				Z-Tests of Proportions		
	Receptive Segment	Balanced Segment	Restricted Segment	Marketing Managers	Receptive Versus Marketing Managers	Balanced Versus Marketing Managers	Restricted Versus Marketing Managers
N	384	801	842	162			
Cookies							
Closed	20.6	25.5	80.6	12.3	2.30	3.63**	17.30**
Permission	66.1	72.9	17.3	82.1	–3.76**	–2.45*	–16.87**
Open	13.1	1.6	2.0	5.6	2.57	–3.12**	–2.65**
Biometrics							
Closed	4.9	10.5	51.2	12.3	–3.08**	–.67	9.12**
Permission	65.9	84.3	40.7	80.2	–3.34**	1.29	–9.22**
Open	29.2	5.2	8.1	7.4	5.55**	–1.11	.30
Loyalty Cards							
Closed	.5	3.4	32.5	7.4	–4.67**	–2.35*	6.48**
Permission	61.7	84.4	53.9	72.8	–2.48*	3.54**	–4.45**
Open	37.8	12.2	13.5	19.8	4.10**	–2.58**	–2.08*
RFID							
Closed	25.8	46.8	80.8	46.3	–4.70**	.12	9.32**
Permission	44.3	47.3	12.0	40.7	.78	1.54	–8.98**
Open	29.9	5.9	7.2	13	4.17**	–3.21**	–2.47*
Text Message							
Closed	38.0	40.4	93.9	46.6	–1.87	–1.46	16.02**
Permission	55.5	59.6	6.1	53.1	.51	1.53	–15.94**
Open	6.5	.0	.0	.0	3.32**	.00	.00
Pop-Up Advertisements							
Closed	36.5	48.3	91.1	35.2	.29	3.05**	16.99**
Permission	48.7	49.3	7.7	53.1	–.94	–.88	–14.81**
Open	14.8	2.4	1.2	11.7	.96	–5.53**	–7.30**
Telemarketing							
Closed	14.6	19.7	73.2	19.1	–1.31	.18	13.18**
Permission	72.1	78.9	25.7	76.5	–1.06	.68	–12.51**
Open	13.3	1.4	1.2	4.3	3.12**	–2.47*	–2.80**
Spam							
Closed	22.1	30.2	84.1	24.7	–.66	1.40	15.89**
Permission	67.4	68.5	14.8	74.1	–1.55	–1.41	–16.10**
Open	10.4	1.2	1.1	1.2	3.69**	.00	–.11

*$p < .05$.
**$p < .01$.

concern. From our data, we learned that for 58.5% of the consumers surveyed, their overall expectations do not differ much from marketing managers. That is, the marketing managers' expectations for privacy boundaries are similar to those of the receptive and balanced consumer segments. However, for the restricted segment (41.5% of consumers), the expectation between marketers and consumers is not in alignment but rather far apart.

We further analyzed the segments by comparing them with marketing managers' preferences for setting privacy boundaries for eight information technologies that have been controversial over the last decade. This situational analysis overcomes previous research that has been criticized for not adequately addressing the context and being cast in too broad of generalities (Solove 2008).

In examining the restricted segment, we found that this segment was strongly against all technologies and wanted much more protection than marketers expected to give. The technologies for which this segment differed most from managers were for cookies, pop-up advertisements, telemarketing, and spam. Though representing 41% of the sample, this segment was less educated and less affluent than other consumers. Note also that though this segment is the most concerned about privacy, it is larger than the fundamentalist group that Westin found. Because of its size, this group drives the overall market perception (without a segmented view) that marketers' values are not aligned with consumers. Marketers might consider educational approaches to this segment of consumers to make them less concerned about the technologies. In addition, public policy should focus on educating this segment about legislation in

place so that they are not deprived of the benefits these technologies provide.

Such educational efforts can begin by informing consumers in the restricted segment of current legislation and regulation that protects their privacy. For example, some of the restrictive segments members may not be aware of the Do Not Call legislation or the CAN-SPAM act. In addition, educational efforts need to help these segment members become aware of the boundary management mechanisms outlined in Table 1. Efforts that teach consumers how to use their browsers to block pop-up advertisements or clear cookies; opt out of specific technologically supported programs that marketers use, such as in the case of text messaging; or sign up and use persistent cookies to block behavioral advertising might provide this segment more control. Currently, there are many online organizations, such as AARP.org, safeshopping.org, and consumerreports.org, that offer suggestions to consumers on how to protect themselves online. The FTC attempts to protect consumers' online privacy by offering games and tutorials on its Web site (www.onguardonline.gov). Moreover, publications could highlight how organizations with strong privacy records use technologies to serve consumers better so that trust levels for this segment might grow. This might be particularly important for marketing efforts using RFID tags and biometrics.

In contrast, the receptive segment possessed a much more liberal view than marketing managers, in that they did not want more protection than marketing managers for any technology. Indeed, they were more experimental and had a higher propensity for allowing newer technologies, such as RFID, text messaging, and biometrics. Demographically, this group was the most educated and affluent, and it is likely that members were more familiar with these technologies. Further research is needed to understand the motivations and efficacy levels behind their propensity for open boundaries.

The impact of educational efforts on this segment depends on members' familiarity with and knowledge of existing regulation and behavioral protection mechanisms. It is plausible that though consumers report that they have knowledge, they may still be misinformed. Additional research is needed to test consumer awareness and behavior of protection mechanisms. For newer technologies such as biometrics, text messaging, and RFID, however, it is possible that educational efforts will make the segment's members more cautious as they become more informed.

For the most part, public policy and self-regulation efforts for the balanced segment, which demographically represented the average of the market, appear to have worked. The overall magnitude of privacy boundary preferences for the balanced segment was fairly aligned with marketing managers. For the heavily regulated technologies of telemarketing and spam, this segment's expectations were not different from marketing managers' expectations. However, differences existed for the less regulated technologies of cookies and pop-up advertisements. For these technologies, the balanced segment wanted more control, and compared with marketing managers, a larger percentage of the balanced segment wanted closed boundaries. For loyalty cards, the balanced segment was more comfortable with permission-based boundaries. For technologies with which consumers are less familiar, such as biometrics and RFID, there was also no difference.

For the balanced segment, educational efforts should be directed to enable the segment members to make informed trade-offs. Thus, information should note both the risks and the benefits to the group participating in marketing information system programs. Self-regulation approaches of informing consumers about how cookies and pop-up advertisements are used in behavioral advertising may work particularly well for this segment. The challenge with regard to disclosure is how to provide information that is concise, informative, relevant, and comprehensible.

Note that the misalignment of the balanced and restricted segments' expectations for cookies and pop-up advertisements is consistent with current regulatory attempts to rein in cookies with respect to behavioral advertising (Miyazaki 2008) and the use of spyware (Cain 2008). For both of these technologies, the information gathering involves covert actions, which when discovered by consumers can result in a backlash (Milne, Bahl, and Rohm 2008). As Miyazaki (2008) notes, further research is needed to understand consumers' knowledge of and reaction to how cookie technology is being used and how this affects their desire for privacy. Such research would be useful in devising approaches for appropriate contextual notification of cookie placements. Alternatively, increases in knowledge help consumers use the tools currently available to opt out or opt in to cookies placement (see Table 1). The scenario we presented in this research described a general cookie usage, in which HTML files could be used to remember passwords or personalize pages. If more intrusive scenarios were shown to consumers—for example, cookies being used to transfer information to third parties in an advertising network—the results might have been even further from managers' expectations. Indeed, recent FTC (2009b) commentary on behavioral advertising has indentified problems with third-party transfers of consumers' information without their knowledge and consent. Likewise, the pop-up advertisement scenario focused on the intrusion and annoyance element of this type of advertisement but did not address that pop-up advertisements can be used to deliver spyware or other unwanted files, such as cookies. The impact of spyware on consumers' expectations for pop-up advertisements is likely to create a higher percentage of closed preferences; the impact on marketers remains an empirical question.

These emergent areas highlight the observation that industry response often lags behind consumer preferences. Research has shown that firms resist regulation, and regulation is not found to be effective unless it is concrete and specific (Lorenzo 2007). In terms of ethical perspectives, marketing managers could improve their positions by being more proactive and self-regulating before they are forced to do so. Marketing managers have the power in this relationship, and theory dictates that it is in managers' interest to align their expectations with those of their consumers. This is because consumers' trust in organizations can be hurt if they learn of the unethical use of new information technologies (Caudill and Murphy 2000). Moreover, from a procedural justice perspective, it is in marketing managers' best

interest to make notice and choice available in formats that consumers expect.

Taken as a whole, this research found that marketers' attempts aligned with expectations of some segments of consumers. It is plausible to expect that there will always be a segment of consumers who are mistrustful of technology and less open to engaging in information exchanges with marketers. For the majority of consumers, however, the overall approach to boundary management seems to be in close alignment with marketing managers' expectations. Yet caution is raised that, in general, expectations are aligned after there has been discussion and pressure brought on the marketing managers by various publics (Peltier, Milne, and Phelps 2009). Thus, we observe that for segments that are more receptive to the managerial use of information, there is concern about unregulated technologies and overstepping the use of the technologies, as we found with cookies. For many of these technologies, there is a lack of understanding, and there is no or little regulation. However, as knowledge increases, concern may grow, and action—either self-regulation or legislative—will need to be taken. When a technology is regulated, the majority of the population will be comfortable with information exchanges that fit within the regulated boundaries. However, there will always be one segment that will choose not to interact with certain information technologies.

Conclusions

Examining privacy boundaries from a more context-specific framework overcomes many of the limitations of previous work. Yet there were limitations in the study, which we now document. First, this study used eight scenarios about marketing technologies to elicit consumers' choices about the type of permission they would prefer from marketers. The results are limited to these technologies; certainly, other new technologies, such as surveillance cameras, global positioning system monitoring, and verichips, could be examined. Second, the scenarios reflect only one view of each of the eight technologies, and we recognize that the wording and the presentation of scenarios can influence the absolute responses. For example, we described only one particular type of cookie and biometric usage. Wording of the scenarios can also create particular biases and make some scenarios seem more favorable than others. With these limitations, we recognize that absolute comparison across scenarios is not reliable. To avoid this problem, we focused on the comparison of the differences between managers and consumers within technologies. Third, the sample sizes for marketing managers and database vendors were small and reflected relatively low response rates. Despite efforts to test for nonresponse bias, we cannot rule out such bias entirely. Further research might want to conduct addition studies with new samples of marketing managers.

In conclusion, this study is one of the few studies that directly compare managers' and consumers' answers with the same set of privacy-related questions. Moreover, it examines privacy expectations from a consumer segment level and for multiple technologies. As new technologies are introduced, it is important for research to track how both sides of the exchange dyad view privacy boundaries. Moreover, with emerging technologies, permission may not fit neatly into opt-in or opt-out formats. Problems are also compounded as more companies adopt integrated marketing communication approaches and share and use consumer data gathered from multiple channels (Peltier, Milne, and Phelps 2009). Figuring out how to gain permission from different consumer segments for new technologies that are not fully transparent to consumers is a much needed area of research.

Appendix: Research Scenarios

1. Companies place cookies in the computers of consumers to track their activity on websites. Cookies help companies learn what websites consumers visited prior to and after they left the website. Some consumers find use of cookies convenient because they personalize the website and help remember passwords. Do you think a company's use of cookies to gather information:
2. A clothing store collects personal identifying information and detailed body measurements (bust, waist, hip size) using a body scanning technology. With this information, stores can customize clothing to fit their customers exactly. The store retains this information in their databases for future use. Do you think storing this information indefinitely in databases:
3. Retail stores issue loyalty cards to customers in order to collect customers' information such as their name, address, phone, e-mail, and other demographics. In exchange for information they offer customers discounts. Only shoppers with cards can get discounted prices. When customers check out, the items are scanned and the information is linked to the loyalty card. Do you think collecting detailed information on customer purchases:
4. RFID tags are being put in products such as clothing to help track the product code for inventory, sales, and returns. A retail store scans the tags of clothes its customers are wearing without them being aware the store is using an RFID reader. This information is used to learn about customer preferences. Do you think collecting information on customers' preferences by scanning RFID tags on their clothes:
5. Companies can send text messages to cell phones. These text message advertisements provide consumers with useful time and place relevant information. However, some consumers find the messages sent to their private cell phone annoying. Do you feel companies sending text messages to cell phones:
6. Companies involved with e-commerce can use popup ads to break through the clutter and attract consumer's attention. Some consumers may feel that the ads are entertaining and provide useful information. While other consumers may find them inconvenient as they have to close the ads by clicking a corner of the ad. Do you think the use of popup ads:
7. Companies who have established business relationships with customers are permitted by law to contact them by telephone at home. These companies are not restricted by the National Do Not Call Service. However, many of these calls occur during inconvenient times. Do you think telemarketing calls by these companies:
8. Companies often find new customers by using email lists. The email messages provide potential customers with product and purchasing information. Some individuals find receiving these unsolicited emails undesirable. Do you think companies sending unsolicited emails:

References

Ackerman, Mark S., Lorrie Faith Cranor, and Joseph Regale (1999), "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," in *Proceedings of the 1st ACM Conference of Electronic Commerce*. New York: Association for Computing Machinery, 1–8.

Altman, Irwin (1975), *The Environment and Social Behavior*. Belmont, CA: Wadsworth.

Ashworth, Laurence and Clinton Free (2006), "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," *Journal of Business Ethics*, 67 (2), 107–123.

Bellman, Steve, Eric J. Johnson, and Gerald L. Lohse (2001), "To Opt-In or Opt-Out? It Depends on the Question," *Communications of the ACM*, 44 (2), 25–27.

Bloom, Paul N., George R. Milne, and Robert Adler (1994), "Avoiding Misuse of New Information Technologies: Legal and Societal Considerations," *Journal of Marketing*, 58 (January), 98–110.

Bosworth, Martin H. (2005), "Loyalty Cards: Reward or Threat?" (July 11), (accessed May 3, 2008), [available at http://www.consumeraffairs.com/news04/2005/loyalty_cards.html].

Burnell, John (2008), "Washington RFID Bill Expected to Become Law Today," (accessed February 9, 2009), [available at http://www.rfidupdate.com/articles/index.php?id=1569].

Cain, Rita Marie (2008), "An Analysis of Spyware Enforcement Actions in the Pursuit of Sound Internet Advertising Policy," in *Marketing and Public Policy Conference Proceedings*, Vol. 18, John Kozup, Charles R. Taylor, and Ronald Paul Hill, eds. Chicago: American Marketing Association, 28–35.

Campbell, Alexandra (1997), "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy," *Journal of Direct Marketing*, 11 (3), 44–57.

CAN-SPAM Act (2003), Pub.L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§7701-7713 and 18 U.S.C. § 1037).

Caudill, Eve M. and Patrick E. Murphy (2000), "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing*, 19 (Spring), 20–26.

Cespedes, Frank V. and H. Jeff Smith (1993), "Database Marketing: New Rules for Policy and Practice," *Sloan Management Review*, 34 (Summer), 7–22.

Children's Online Privacy Protection Act (1998), 15 U.S.C. §§ 6501-6506, P.L. No. 105-277, 112 Stat. 2681-728.

Computer Spyware Act (2005), Title 19 Rev. Code Washington.

Consumers Against Supermarket Privacy Invasion and Numbering (2008), (accessed May 3, 2008), [available at http://www.nocards.com].

Culnan, Mary J. (1993), "How Did They Get My Name? An Exploratory Examination of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*, 17 (3), 341–63.

——— (2000), "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing*, 19 (Spring), 20–26.

——— and Pamela K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10 (1), 104–115.

Derlega, Valerian J. and Alan L. Chaikin (1977), "Privacy and Self-Disclosure in Social Relationships," *Journal of Social Issues*, 33 (3), 102–115.

Direct Marketing Association (2009), "Privacy," (accessed March 1, 2009), [available at http://www.the-dma.org/privacy/].

——— (2010), "Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary," (accessed February 15, 2010), [available at http://www.the-dma.org/guidelines/onlineguidelines.shtml].

Dixon, Pam (2008), "Consumer Tips: How to Opt-Out of Cookies That Track You," (accessed May 1, 2008), [available at http://www.worldprivacyforum.org/cookieoptout.html].

Dolnicar, Sara and Yolanda Jordaan (2007), "A Market-Oriented Approach to Responsibly Marketing Information Privacy Concerns in Direct Marketing," *Journal of Advertising*, 36 (Summer), 123–49.

Findbiometrics.com (2009), "EU Approves Biometric Passports," (January 15), (accessed February 9, 2009), [available at http://www.findbiometrics.com/articles/i/6095/].

FTC (2003), "Telemarketing Sales Rule, Final Amended Rule," *Federal Register*, 68 (19), 4580–4679.

——— (2005), "Radio Frequency Identification: Applications and Implications for Consumers," a Federal Trade Commission Workshop Report, (March), (accessed June 16, 2009), [available at http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf].

——— (2007), "FTC Staff Proposes Online Behavioral Advertising Privacy Principles," (accessed December 20, 2007), [available at http://www.ftc.gov/opa/2007/12/principles.shtm].

——— (2009a), "The CAN-SPAM Act: A Compliance Guide for Business," (September), (accessed February 15, 2010), [available at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm].

——— (2009b), "FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising," (accessed February 18, 2009), [available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf].

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 10 (Spring), 149–66.

Holtzman, David (2006), *Privacy Lost: How Technology Is Endangering Your Privacy*. San Francisco: Jossey-Bass.

Hoy, Maria Grubb and Joseph Phelps (2003), "Consumer Privacy and Security Concerns on Church Web Sites," *Journal of Public Policy & Marketing*, 22 (Spring), 58–70.

Hunt, Shelby D., Richard Sparkman, and James B. Wilcox (1982), "The Pretest in Survey Research: Issues and Preliminary Findings," *Journal of Marketing Research*, 19 (May), 269–73.

Kelly, Eileen P. and G. Scott Erickson (2005), "RFID Tags: Commercial Applications vs. Privacy Rights," *Industrial Management and Data Systems*, 105 (5–6), 703–713.

Krishnamurthy, Sandeep (2001), "A Comprehensive Analysis of Permission Marketing," *Journal of Computer Mediated Communications*, 6 (2), (accessed January 29, 2010), [available at http://jcmc.indiana.edu/vol6/issue2/krishnamurthy.html].

Kumaraguru, Ponnurangam and Lorrie Faith Cranor (2005), "Privacy Indexes: A Survey of Westin's Studies, CMU-ISRI-5-13," Institute for Software Research International, Carnegie Mellon University.

Langenderfer, Jeff and Stefan Linnhoff (2005), "The Emergence of Biometrics and Its Effect on Consumers," *Journal of Consumer Affairs*, 39 (2), 314–38.

Lorenzo, Vincent Di (2007), "Business Ethics: Law as a Determinant of Business Conduct," *Journal of Business Ethics*, 71 (3), 275–99.

Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective," *Journal of the Academy Marketing Science*, 35 (4), 572–85.

McCoy, Scott, Andrea Everard, Peter Polak, and Dennis F. Galletta (2007), "The Effects of Online Advertising," *Communications of the ACM*, 50 (3), 84–88.

Milne, George R. (1997), "Consumer Participation in Mailing Lists: A Field Experiment," *Journal of Public Policy & Marketing*, 16 (Fall), 298–309.

———, Shalini Bahl, and Andrew J. Rohm (2008), "Toward a Framework for Assessing Covert Marketing Practices," *Journal of Public Policy & Marketing*, 27 (Spring), 57–62.

——— and Maria Eugenia Boza (1998), "A Business Perspective on Database Marketing and Consumer Privacy Practices," Marketing Science Institute Report No. 98-110.

——— and ——— (1999), "Consumers' Trust and Concern about Organizations Use of Personal Information in Direct Marketing," *Journal of Interactive Marketing*, 13 (Winter), 7–24.

——— and Mary J. Culnan (2002), "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Sweeps," *The Information Society*, 18 (5), 345–60.

——— and Mary Ellen Gordon (1994), "A Segmentation Study of Consumers' Attitudes Toward Direct Mail," *Journal of Direct Marketing*, 8 (Spring), 45–52.

——— and Andrew Rohm (2000), "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives," *Journal of Public Policy & Marketing*, 19 (Fall), 238–49.

Miyazaki, Anthony (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Cookie Trust and Anticipating Patronage," *Journal of Public Policy & Marketing*, 27 (Spring), 19–33.

——— and Ana Fernandez (2000), "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*, 19 (Spring), 54–61.

——— and ——— (2001), "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs*, 35 (1), 27–45.

O'Connor, Mary Catherine (2008), "EC Publishes RFID Privacy Policy Draft," *RFID Journal*, (February 22), (accessed April 28, 2008), [available at http://www.rfidjournal.com/article/articleprint/3940/-1/1/].

Peltier, James W., George R. Milne, and Joseph E. Phelps (2009), "Information Privacy Research: Framework for Integrating Multiple Publics, Information Channels, and Responses," *Journal of Interactive Marketing*, 23 (2), 191–205.

Peslak, Alan (2005), "An Ethical Exploration of Privacy and Radio Frequency Identification," *Journal of Business Ethics*, 59 (4), 327–45.

Petronio, Sandra (2002), *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

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

Regan, Priscilla (1995), *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.

Roznowski, JoAnn L. (2003), "A Content Analysis of Mass Media Stories Surrounding the Consumer Privacy Issue 1990-2001," *Journal of Interactive Marketing*, 17 (2), 52–69.

Sarathy, Ravi and Christopher J. Robertson (2003), "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics*, 46 (2), 111–26.

Sheehan, Kim B. (2005), "In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites," *Journal of Public Policy & Marketing*, 24 (Fall), 273–83.

Smith, H. Jeff (1994), *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press.

Smith, N. Craig and Elizabeth Cooper-Martin (1997), "Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability," *Journal of Marketing*, 61 (July), 1–20.

Smith, Robert Ellis (2000), *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Privacy Journal.

Solove, Daniel J. (2008), *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Telephone Consumer Protection Act (1991), 47 U.S.C. 227.

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

Xu, Heng, Tamara Dinev, H. Jeff Smith, and Paul Hart (2008), "Examining the Formation of Individual's Privacy Concerns: Toward and Integrative View," in *ICIS 2008 Proceedings*, Paper 6, (accessed February 3, 2010), [available at http://aisel.aisnet.org/icis2008/6/].