Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage

Anthony D. Miyazaki

The use of Internet cookies by visited Web sites and third-party firms has been criticized by consumer advocates, policy makers, and even marketers themselves as a potential threat to consumer privacy. However, surprisingly little research has examined how the interactive effects of the disclosure and practice of cookie use as a method of nonconsensual identification might influence online users' affect or behavior. The current research addresses this lack of research by presenting the results of three studies. Study 1, a longitudinal examination of the online environment from 2000 to 2007, finds that both cookie use and disclosure have increased, but the covert use of cookies is still a concern. Study 2 finds that consumers' negative reactions to cookie use are significantly reduced by a priori cookie disclosure by the visited Web site. Study 3 shows that consumers' online experience and desire for privacy act as additional moderators of reactions to cookie use. The author examines the implications of the three studies from the perspectives of research, management, and public policy.

Keywords: covert marketing, privacy, disclosure, information disclosure, Internet, cookies, trust, e-commerce

Consider a consumer who has a gambling or other addiction problem and decides to search online for various programs or literature regarding treatment. That same consumer also visits several investment, credit card, or banking Web sites that might suggest a particular income, debt, or wealth level. The consumer also logs on to assorted social networking sites that have collected and stored demographic and socioeconomic information. Now consider that a third party has access to these visits, searches, and information, either by surreptitiously gathering data as the consumer surfed the Internet or by participating in information sharing with the various Web sites visited. When the third party sells the collective information to various marketers, is there the potential for these firms to make offers that take advantage of the addictive nature, monetary situation, and personal state of this consumer? Would the consumer have acted in the same way if this nonconsensual identification was made more apparent?

As various aspects of online activity continue to grow at a rapid pace, online privacy remains a key focus of consumer advocates and public policy makers (Federal Trade Commission [FTC] 2000, 2007; Milne 2000; Milne, Rohm, and Bahl 2004). Although concerns range from worries about how marketers will use information provided by online users to privacy-related security issues, a large concern is the nonconsensual identification and surveillance of online users by the sponsors of the Web sites they visit and by third-party organizations (Antón, He, and Baumer 2004; Cranor, Guduru, and Arjula 2006; FTC 2000; Ha et al. 2006; Leibrock 1997; Milne, Rohm, and Bahl 2004; Miyazaki and Fernandez 2000; Sheehan 2005). Such online nonconsensual identification is often carried out as a covert marketing activity by the surreptitious use of cookie files (explained in more detail in the following section). This is despite FTC guidelines and consumer distaste for nonconsensual identification and is due in great part to consumers' paucity of knowledge regarding cookie functions and their ubiquitous usage. Thus, a lack of cookie disclosure has been, and still remains, an important facet of consumer online privacy. Moreover, as Milne, Bahl, and Rohm (2008) note, the lack of disclosure regarding whether and how cookies are used to gather information is a covert marketing practice that may harm consumer trust and patronage.

The public policy of online privacy can be discussed from a social contract theory perspective (Dunfee, Smith, and Ross 1999), whereby provision of consumer information is expected to yield a certain responsibility (i.e., in the form of an implied social contract) of the receiving organization to collect and care for such information in a responsible manner. Indeed, prior researchers have been in agreement that when marketers collect information from consumers without their awareness, an implied social contract is breached (Culnan 1995; Milne and Gordon 1993; Phelps, Nowak, and Ferrell 2000). These implied social contracts are derived from social norms (Caudill and Murphy 2000) that may be influenced by prior behavior,

Anthony D. Miyazaki is Knight Ridder Research Professor and Associate Professor of Marketing, College of Business Administration, Florida International University (e-mail: miyazaki@fiu.edu).

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

Vol. 27 (1) Spring 2008, 19–33

explicit contractual agreements, or industry and governmental regulation. The breaking of such an implied social contract is expected to result in lower consumer trust, less favorable affect toward the culpable party, and, thus, less likelihood of future patronage.

With respect to the information-gathering and -usage facets of online privacy, the FTC's guidelines regarding consumer choice with respect to what and how information will be gathered address this implied social contract. However, consumers cannot make choices regarding information provision if they do not have knowledge of an organization's information-gathering practices. This is the rationale behind the FTC (2000, p. iii) guideline of "notice," which states that consumer-oriented commercial Web sites are "required to provide consumers clear and conspicuous notice of their information practices," such as how information is collected, including "non-obvious means such as cookies." These Web sites are also required to disclose any information provision to third parties, regardless of whether that information is passed on to a third party or the third party accesses the information directly through the Web site.

Thus, the implied social contract held in the minds of online consumers suggests that breaches of this contract, such as the undisclosed use of cookies, could be detrimental to consumer attitudes toward the information-gathering practice and the Web site or firm as well. At the same time, it is not clear under which conditions consumers may believe that cookie use or, more specifically, the lack of explicit disclosure of cookie use constitutes a violation of the social contract. Thus, factors such as consumers' desire for privacy and their degree of online experience come into play.

From a strict policy perspective, although any covert practice of online consumer identification is in violation of FTC (2000) guidelines, surprisingly little research has examined the practice of nonconsensual consumer identification or its effects on consumer attitudes and intended behavior. This research remedies this deficiency by presenting (1) a longitudinal examination of how cookie disclosure and usage among top Web sites has changed during the past seven years; (2) two experimental studies that examine online user reaction to disclosure versus practice of this method, as well as moderators of those reactions; and (3) implications for policy makers, online organizations, and consumers.

Cookies

The most common method of identifying and tracking online consumer activity involves the placement of small text files on a consumer's hard drive that are then offered back to the Web site during subsequent visits by the consumer (Bayan 2001; Gralla 2007; Linn 2005; Millett, Friedman, and Felten 2001). These text files, or "cookies" as they are commonly called, can be designed to persist on the user's hard drive for only the current online session; they can be configured to last for days, months, or years; or they essentially can be designated to last indefinitely. Although they have continually been a concern with respect to online privacy (e.g., Cranor 1999; FTC 2000; Jackson et al. 2006; Milne, Rohm, and Bahl 2004; Palmer 2007; Reagle and Cranor 1999), cookies in and of themselves do not constitute violation of an online user's privacy. Indeed, many Web sites require cookies to operate effectively. For example, online shopping sites that store items in a virtual shopping cart require the placement of cookies on the shopper's hard drive to identify the shopper as the individual who stored those particular items (Chapman and Dhillon 2002). However, cookies can constitute an invasion of privacy from several perspectives—namely, their ability to track user information and behavior; their use by third parties; their covertness; their duration and ubiquity; and consumers' lack of information regarding their usage, degree of threat, and control.

Tracking User Information and Behavior

The placement of cookies on an Internet user's hard drive can be accomplished in several ways—for example, by using Web bugs (also referred to as Web beacons, pixel tags, and clear graphic interchange formats [GIFs]) to set the cookie from either the visited Web site or a third-party site (Bayan 2001; Martin, Wu, and Alsaid 2003). Regardless of the initial method of placement, the purpose of a cookie is to record some aspect of online user information—from relatively innocuous data, such as the user moving from a particular Web page, to more private personally identifiable information or passwords—for later retrieval (Chapman and Dhillon 2002; Reagle and Cranor 1999). The information recorded can be explicit information provided by the Internet user (e.g., gender, age, zip code, account numbers), behavioral information regarding user movement from one Web page to the next (including time, duration, and sequence of Web movement), or the tracking of how many times a particular banner ad has appeared during an online session (Martin, Wu, and Alsaid 2003; Raghu, Rao, and Whinston 2001).

This information has been of great value to marketers in helping create user profiles to assist in targeting advertisements and product offerings (Caudill and Murphy 2000; Martin, Wu, and Alsaid 2003; Raghu, Rao, and Whinston 2001). Although much information acquired through cookie use is not directly personally identifiable information, the ability to aggregate various profiles creates the opportunity for such information to become personally identifiable and, as such, has been shown to be a cause of concern to online consumers (Chellappa and Sin 2005). Unfortunately, recording of such information may constitute an invasion of privacy, depending on the degree of disclosure that accompanies this activity (Caudill and Murphy 2000; Miyazaki and Fernandez 2000; Sheehan 2005). Concerns about this type of information tracking have been raised by technology experts (Berghel 2002; Cranor 1999, 2002), privacy advocates (Dixon and Givens 2004; King 2001), researchers (Caudill and Murphy 2000; Milne 2000; Miyazaki and Fernandez 2001; Sheehan 2005), and government organizations (Department of Transportation 2003; FTC 2000; United States Courts 2000).

Third-Party Cookie Use

Although the general use of cookies by visited Web sites is a concern of consumers and policy makers alike, perhaps a deeper concern involves the use of cookies placed on the

Internet user's hard drive by a party not directly visited by the online consumer. Such "third-party cookies" are often sanctioned by the visited Web site to build consumer profiles by the third-party organization for targeted marketing purposes (Lavin 2006; Raghu, Rao, and Whinston 2001). Commercial firms, most notably DoubleClick and more recently JetBlue, have been formally chastised for their reliance on or allowance of third-party cookies (Antón, He, and Baumer 2004; Chapman and Dhillon 2002; Hemphill 2000).

Third-party cookies have also caught the attention of the FTC, whose examination of Web sites conducted in February and March 2000 found that 57% of sites in a random-sample group (N = 335) and 78% of the busiest U.S. sites (N = 91 of the 100 busiest sites) allowed cookie placement by third parties. Concerns about third-party cookies have been reiterated over the years in terms of how they are implemented (Martin, Wu, and Alsaid 2003), their lack of control by the consumer (Berghel 2002), and the possible circumvention of modern browser privacy settings by cooperative actions of offending Web sites (Jackson et al. 2006).

Covertness of Cookie Use

Another concern regarding cookie placements is the covert nature of their usage. The placement of third-party cookies is often facilitated by the use of "clear GIFs" that are only one pixel by one pixel in size, which essentially makes them invisible to the consumer (Hoofnagle 2005; Martin, Wu, and Alsaid 2003). The FTC (2000) described cookies as a "nonobvious" means of information collection and their undisclosed use as a clear violation of the notice aspect of fair information practices. Indeed, even when Web sites disclose the general use of cookies (whether for Web site effectiveness, targeted offers, and so forth), the lack of explicit disclosure of any cookies placed by third parties is still considered a privacy violation (Antón, He, and Baumer 2004).

Modern Web browsers are now equipped to provide consumers with the ability to reject or delete cookies in accordance with their privacy preferences (Linn 2005). However, several studies have shown that many consumers do not take advantage of these capabilities (Ha et al. 2006; Jensen, Potts, and Jensen 2005; Milne, Rohm, and Bahl 2004). Moreover, browsers do not allow users to understand when the cookies that persist on their hard drives are actually used (in essence, retrieved rather than set) by visited Web sites and how the retrieving Web sites use them (Lederer et al. 2004; Millett, Friedman, and Felten 2001).

Cookie Prevalence and Persistence

Cookies are the most common method of identifying and compiling information regarding Web users (Bayan 2001; Gralla 2007; Ha et al. 2006; Linn 2005; Martin, Wu, and Alsaid 2003). Estimates of cookie use by Web sites vary, but they are often high (particularly among commercial Web sites), with field studies reporting cookie use from 36% to 100% of sites examined (Hoy and Phelps 2003; Jamal, Maier, and Sunder 2005; Martin, Wu, and Alsaid 2003).

Cookies can also be present on a consumer's hard drive for a significant duration of time. Although some "session cookies" are designed to last only for the duration of the current online session, other "persistent cookies" are set to last for months or years, some clearly far beyond the life cycle of the computer on which they reside (Hoofnagle 2005; Linn 2005). Although informed users now have the capability of removing cookies, there are complaints that expiration dates cannot be easily altered (Millett, Friedman, and Felten 2001). In addition, Sit and Fu (2001) complain that even when the cookie-setting server specifies an expiration date, there is no guarantee that the Web browser being used to access the Internet will delete the cookie. Finally, the encoded nature of many cookies prohibits consumers from knowing which cookies to delete to enhance privacy protection and which to save to aid in online functional efficiency.

Lack of Consumer Knowledge

The final perspective from which cookies serve as a problematic concern with respect to online consumer privacy is the general lack of consumer knowledge regarding cookie functions, their degree of threat to privacy, and how to manage them. For example, prior research has reported not only that online consumers are often confused about the advantages and disadvantages of cookies but also that most cannot properly identify what a cookie is (Ha et al. 2006; Hoofnagle 2005). Indeed, Jensen, Potts, and Jensen (2005) report that though a vast majority (90.3%) of their experienced Internet user sample claimed to have knowledge of cookies, further probes indicated that only 15.5% of those making that claim demonstrated even simple cookie knowledge.

This apparent overconfidence suggests that consumers may have limited capability to deal effectively with the potential for cookie-related invasions of privacy. Indeed, evidence suggests that most consumers do not use available technology to prohibit cookies from being placed on their hard drives (Ha et al. 2006; Jensen, Potts, and Jensen 2005; Milne, Rohm, and Bahl 2004).

Research Issues

Survey research shows that consumers are concerned about nonconsensual identification practices of Web site organizations. Government and industry responses to these consumer concerns have been focused on disclosure of identification practices with the intention that such disclosure removes covert status and facilitates some degree of agreement. The FTC (2000) has made it clear in its discussion and studies of the online environment that the use of undisclosed cookies constitutes a violation of its fair information practice of notice. Indeed, since that time, concerns continue to be raised as to whether levels of disclosure regarding online privacy are sufficient, with recent studies finding considerable deficiencies in full disclosure (Hoy and Phelps 2003; Schwaig, Kane, and Storey 2005).

With respect to cookie placement, recent studies have shown a lack of congruence between cookie use and cookie disclosure both for commercial sites (FTC 2000) and for nonprofit sites (Hoy and Phelps 2003). The potential for such a discrepancy between disclosure and practice may be due to online organizations' concerns that disclosing identification practices will lead to higher levels of privacy concerns by consumers and ultimately lower patronage or

usage rates. Indeed, these organizations may assume that consumers' lack of awareness of cookie usage negates the need for a priori disclosure. However, the advent of software capabilities that enhance consumer knowledge of attempts to place cookies suggests that greater congruence between practice and disclosure could be beneficial to Web site organizations. Unfortunately, no research has directly assessed consumer response to the disclosure of online consumer identification practices in conjunction with variations in consumer knowledge of such practices.

This article responds to this need for research by examining the degree of congruence between Web site disclosures and Web site practices with respect to the use of cookies to identify online patrons (Study 1). This longitudinal investigation (which compares 2000 and 2007) of popular Internet Web sites sets the stage for two experimental studies that assess how consumer detection of nonconsensual identification practices (i.e., the use of cookies) affects consumer trust of the Web site and anticipated patronage decisions. These effects are examined in conjunction with disclosure (Study 2) and with respect to consumers' Internet experience and desire for privacy (Study 3).

Study 1: Market Examination of Cookie Disclosure Versus Usage

Prior investigations of cookie usage have provided individually static representations of the state of practice versus disclosure. Nevertheless, it appears that both Web site cookie use and disclosure in the United States have risen over time. Table 1 presents pertinent results from prior studies that have examined both cookie disclosure and usage. However, none of the studies presented in Table 1 have examined both cookie usage and disclosure of original domain and third-party cookies across a similar sample over time. Such a longitudinal examination would be useful in understanding how the FTC studies and reports have potentially influenced online practices. To fill this gap in the literature, this study compares the cookie usage and disclosure of top Web sites in 2000 and 2007.

Although no formal hypotheses are presented regarding how cookie usage and disclosure have changed over time, several research questions are apparent. These stem from changes in technology, consumer perceptions, and government involvement. For example, from 2000 to 2007, the increase in technological advances in cookie placement and usage (Linn 2005), as well as the acceptance of cookie usage in the online industry (Gralla 2007), suggests an increase in the percentage of top Web sites that use both first-party, or "original domain," cookies (i.e., those set by the visited Web site) and third-party cookies (i.e., those set by a third party that is often unknown to the online consumer). It also suggests an overall increase in the average number of cookies (original domain and third party) placed by Web sites. Conversely, factors such as FTC involvement in online privacy issues, legislation regarding privacy-related activities, and reports of consumer concern about privacy issues suggest that Web site disclosure of both types of cookie use will increase as well. Of particular interest is whether the prevalence of covert cookie placement (i.e., without disclosure) has decreased significantly, particularly for third-party cookies. Thus, the research questions that Study 1 attempts to answer are as follows: Has the prevalence of general and third-party cookie use among popular Web sites changed from 2000 to 2007? Has mean cookie use by individual Web sites increased? Has the disclosure of cookie usage increased during this period? and Has the prevalence of covert cookie use decreased? In light of these questions and the previous discussion, for 2000 and 2007, Study 1 examines (1) the prevalence of general

Table 1. Prior Studies Examining Cookie Practice and/or Disclosure

Study	Date of Data Collection	Sample Information	U_C%	U_3%	D_C%	D_3%
Miyazaki and Fernandez (2000)	January/February 1999	381 random e-commerce Web sites from Excite, Yahoo, and Netscape shopping portals			23[a]	
FTC (2000)	February/March 2000	335 random e-commerce Web sites		57		22
FTC (2000)	February/March 2000	91 of 100 busiest Web sites		78		51
Jamal, Maier, and Sunder (2003)	July 2001	100 of top 500 busiest Web sites	98	79	91	76
Jamal, Maier, and Sunder (2005)	May/June 2002	56 U.K. high-traffic Web sites	88	50	80	96
Hoy and Phelps (2003)	May/June 2002	102 random church (noncommercial) Web sites	36	20	0	0
Sheehan (2005)	March 2004	94 direct-to-consumer branded drug Web sites			90	85[b]

[a]23.1% customer identification (mainly cookie use) disclosure (ranging from 0% to 64.3% across 17 shopping categories).
[b]Disclosed provision of information to third parties.
Notes: U_C = percentage of sample using cookies. U_3 = percentage of sample using third-party cookies. D_C = of those using cookies, percentage disclosing general cookie use. D_3 = of those using third-party cookies, percentage disclosing third-party cookie use (third-party information gathering).

cookie use, (2) the prevalence of third-party cookie use, (3) the amount of (mean) cookie use, and (4) the disclosure of information-gathering practices, particularly for general and third-party cookie use.

Study 1 Methods

To determine which Web sites would be examined, the Media Metrix 500 for January 2000 was accessed in March 2000 and used as a starting point for Web site selection. At that time, the Media Metrix 500 was a publicly accessible list of the 500 Web sites that attracted the most unique (i.e., unduplicated) visitors during the month of measurement. (Because of various changes in firm ownership, this list is no longer publicly available [for a more detailed explanation, see Milne, Culnan, and Greene 2006].)

The first wave of data collection was conducted in June 2000, one month after the FTC released its report to congress on online privacy and fair information practices (FTC 2000). The analyses were limited to .com and .net Web sites because these were the key commercial sites, particularly at that time. Of the 500 Web sites on the list, 58 were not evaluated because they were inaccessible (15), foreign (5), or .edu (18), .gov (14), .org (4), or .mil (2) sites. The second wave of data collection was conducted in February 2007. Over the span of almost seven years, 36 of the original 442 Web sites ceased operations, resulting in a sample size of 406. The comparisons between 2000 and 2007 are based on these 406 Web sites (cf. Milne, Culnan, and Greene 2006).

Each data collection wave proceeded in two stages, one for cookie disclosure and one for cookie practice. Cookie disclosure was investigated by first printing the home page and privacy policy (if any) for each of the Web sites in the sample. Each Web site was assessed for (1) whether it had a privacy policy or privacy statement and (2) whether the policy was directly linked from the Web site home page. Each privacy policy was then examined to determine whether it (3) disclosed general cookie usage, (4) disclosed third-party cookie usage, and/or (5) discussed general information gathering (cf. FTC 2000). To count as third-party cookie disclosure, the privacy policy needed to mention that third parties (e.g., other organizations, ad servers) would or may set or use cookies. Merely mentioning that third parties may collect information was not considered a disclosure of third-party cookies. Two trained research assistants coded each Web site separately. The results between the two sets of codes were then compared (total initial agreement of 95.6% for 2000 and 93.1% for 2007), and any discrepancies in coding were resolved by discussion with the author.

Cookie practice was examined by setting a Web browser (Netscape Navigator) to warn when a cookie was to be placed onto the hard drive. (Current popular Web browsers have similar abilities to detect and warn of cookie placement. Netscape was chosen because during the 2000 data collection, it provided what was believed to be the clearest presentation of cookie information. Netscape was used for the 2007 data collection for consistency, but any of the major Web browsers would have provided similar information.) This resulted in a pop-up window being activated for each cookie that was to be set. If no cookies were found on the home page, up to five other pages were examined, including an order page, if one existed, to check for cookies. Before allowing the cookie to be set, a researcher noted whether the cookie was an original domain server cookie (i.e., it was originated and sent back to the visited Web site) or a third-party cookie. (Cookies that were placed by domains that were clearly related to the original domain were not considered third-party cookies. For example, a cookie set by Americanexpressvacations.com when visiting the Americanexpress.com Web site would not be considered a third-party cookie. The result is a more conservative estimate of third-party cookies than if every nonoriginating cookie was counted as a third-party one.) The originating page for the cookie was also noted (i.e., the home page, ordering page, or other page), as was the cookie expiration date.

Study 1 Results and Discussion

The results from the two waves of data collection appear in Table 2 and reveal no statistically significant difference in the percentage of Web sites with privacy policies in 2000 (83.0%) versus 2007 (86.7%; $Z = 1.47$, not significant [n.s.]). As expected, the percentage of Web sites practicing general cookie use increased from 2000 (81.3%) to 2007 (95.3%; $Z = 6.38$, $p < .01$). This increase was accompanied by an increase in the proportion of Web sites that disclosed cookie usage (from 65.5% to 84.5%; $Z = 5.95$, $p < .01$). Indeed, the overall percentage of Web sites covertly placing cookies decreased from 28.0% in 2000 to 14.8% in 2007 ($Z = 4.68$, $p < .01$).

For third-party cookies, the increase in Web site usage was seemingly more noticeable, from 32.5% in 2000 to 50.2% in 2007 ($Z = 5.22$, $p < .01$). Fortunately, this increase was accompanied by an increase in the proportion of third-party cookie disclosure, from 31.8% of sites using third-party cookies in 2000 to 63.2% in 2007 ($Z = 5.96$, $p < .01$). However, this increase in disclosure was not sufficient to reduce the overall percentage of Web sites that covertly used (or allowed the use of) third-party cookies: 22.2% in 2000 and 18.5% in 2007 ($Z = 1.31$, n.s.).

Finally, there was a notable change over the seven-year period in the number of cookies that each Web site used. For Web sites that had at least one cookie placed on their home page, the average number of cookies on the home page rose from 2.45 in 2000 (range from 1 to 12) to 8.71 in 2007 (range from 1 to 59), a significant increase ($t = 11.8$, $p < .01$). Similarly, the average number of third-party home page cookies grew from 1.57 (range from 1 to 6) to 3.84 (range from 1 to 28), again a significant increase ($t = 4.66$, $p < .01$).

Overall, Study 1 demonstrates that cookie use, both in general and for third-party cookies, has increased significantly over the past seven years. Fortunately, the disclosure of cookie use has also increased to the point that the covert use of cookies (i.e., the use of undisclosed cookies) has decreased for general cookie-setting activity. However, for third-party cookies, there has been no significant decrease in covert cookie use over the past seven years. Finally, the average number of cookies placed on the home page of each of these sites has increased more than threefold, and the number of third-party cookies has more than doubled. These findings of increased cookie use and a lack of

Table 2. Study 1: Web Site Cookie Disclosure Versus Practice for 2000 and 2007

	2000	2007	Test Statistic
Number of Web Sites Examined (N)	406	406	
% of sample (N) with privacy policy	83.0	86.7	Z = 1.47, n.s.
% of Sample (N) Using Cookies (N_C)	81.3	95.3	Z = 6.38, $p < .01$
% of N_C disclosing cookie use	65.5	84.5	Z = 5.95, $p < .01$
% of N_C disclosing general information gathering	80.9	87.1	Z = 2.24, $p < .05$
% of N_C with privacy policy	86.1	87.9	Z = .71, n.s.
% of N covertly placing cookies	28.0	14.8	Z = 4.68, $p < .01$
% of Sample (N) Using Third-Party Cookies (N_{3PC})	32.5	50.2	Z = 5.22, $p < .01$
% of N_{3PC} disclosing third-party cookie use	31.8	63.2	Z = 5.96, $p < .01$
% of N_{3PC} disclosing general information gathering	76.5	85.3	Z = 1.98, $p < .05$
% of N_{3PC} with privacy policy	83.3	85.3	Z = .48, n.s.
% of N covertly placing third-party cookies	22.2	18.5	Z = 1.31, n.s.
For Web Sites with Any Cookies on Home Page			
Average number of cookies on home page	2.45	8.71	t = 11.8, $p < .01$
For Web Sites with Any Third-Party Cookies on Home Page			
Average number of third-party cookies on home page	1.57	3.84	t = 4.66, $p < .01$

decreased third-party covert use warrant the need to examine consumer response to cookie use in light of variations in disclosure, desire for privacy, and Internet experience. Studies 2 and 3 examine these issues.

Study 2: Trust Effects of Cookie Disclosure Versus Usage

Study 1 demonstrates the growing pervasiveness of cookies, but it also shows that a large portion of frequently visited Web sites are lacking in terms of disclosure. Moreover, prior examinations of cookie disclosure versus practice suggest that less heavily trafficked Web sites are even more likely to violate privacy principles by the undisclosed use of cookies (e.g., FTC 2000). From a consumer perspective, such violations of privacy breach the implied social contract between the consumer and the Web site organization (Dunfee, Smith, and Ross 1999), which is likely to harm the organization's reputation and generate privacy concerns. Prior work has shown that both privacy concerns and damaged reputation can lead to lower perceptions of trust (Jarvenpaa, Tractinsky, and Vitale 2000; Jutla and Bodorik 2005; McKnight, Choudhury, and Kacmar 2002). This follows accepted definitions of trust as being "a willingness to rely on an exchange partner in whom one has confidence" (Moorman, Deshpandé, and Zaltman 1993, p. 82) and as having "confidence in the exchange partner's reliability and integrity" (Morgan and Hunt 1994, p. 23). Such losses of reputation and trust, as well as enhanced privacy concerns, have also been shown to result in lower usage, adoption, and patronage intentions (Chellappa and Sin 2005; Jarvenpaa, Tractinsky, and Vitale 2000; Jutla and Bodorik 2005). Thus, although consumers would be expected to view the use of cookies negatively (as several survey studies mentioned previously have indicated), such an effect would be exacerbated by the absence of reasonable disclosure. Thus, the following interactive hypothesis is put forth:

H_1: Web site disclosure and consumer detection of a covert identification practice (i.e., an attempt to place a cookie) interact such that when disclosure is absent, consumer detection negatively affects (a) consumer trust, (b) usage intentions, and (c) user recommendations; however, when disclosure is present, such effects are attenuated or eliminated.

Study 2 Methods

Study 2 used a 2×2 between-subjects experimental design that manipulated Web site disclosure of cookies (absent versus present) and the Web site practice of setting cookies (used versus not used). The experimental setting involved a ruse, in which participants were asked to evaluate a Web site that a local firm was considering to use as an intermediary to sell elementary school uniforms to parents. The setting was pretested and found to be one of interest to local parents and one that required a relatively high degree of trust from the parents with respect to the Web site organization.

Participants were adults recruited at a local outdoor town gathering of a suburb of a large metropolitan area and were screened to ensure that each had a child in one of the suburb's schools (public or private) and had made at least one purchase online within the prior 12 months. Participants were presented with a new $2 bill for participating in the study and were entered into a drawing for four $25 prizes.

Each participant was asked to sit at a laptop computer and fill out a short questionnaire before evaluating the Web site. The questionnaire presented seven items that included a three-item measure ($\alpha = .84$) of general online shopping risk (Miyazaki and Fernandez 2001). The other items included whether participants ever purchased school uniforms (a requirement for even the local public elementary school [81%]), whether they had made a purchase online within the past 12 months (100%), whether they had a child in any of the suburb's schools (100%), and whether they

were members of any of the local parent–teacher–student associations (46%). These items were included to help with the ruse of the experimental procedure and to ensure that the screening had been accomplished correctly.

After completing the preliminary questionnaire, participants were asked to spend the next five minutes evaluating a Web site and were told that they could exit the browser (by clicking the red "x" in the upper-right-hand corner) when they were ready to complete the remainder of the survey. They were then taken immediately to the faux school-uniform Web site home page, which included a short privacy statement at the bottom of the page (visible within the frame of the computer screen without scrolling). This privacy statement included the manipulation for the cookie disclosure (the first of the two independent variables). The cookie-disclosed statement read as follows:

> When you use certain services at our Web site, we may ask you to provide personally identifying information. The information we collect from you may be combined with other information obtained by our other divisions or by partner companies. But we'll only do this with your permission. Also, to enhance your experience with our Web site, we use "cookies" and other technologies. Cookies are small text files placed via your computer's browser. They store your preferences and how you move through our site and help us meet your needs. Please be assured that your privacy is always our biggest concern.

The cookie-undisclosed statement was designed to be approximately the same length but without the cookie disclosure:

> When you use certain services at our Web site, we may ask you to provide personally identifying information. The information we collect from you may be combined with other information obtained by our other divisions or by partner companies. But we'll only do this with your permission. Also, to enhance your experience with our Web site, we use many advanced technologies. These technologies help you operate our Web site. They also combine with your browser so you can move through our site and they help us meet your needs. Please be assured that your privacy is always our biggest concern.

The privacy statement was purposely kept short (under 100 words) and at a relatively low reading level (approximately 10.5 on the Flesch–Kincaid scale) so that the cookie disclosure information would be seen and understood. This compares with Milne, Culnan, and Greene's (2006) findings that top-ranked Web site privacy policies average 1950 words, with an average Flesch–Kincaid grade-level score of 12.3.

Participants were then able to click on several links that showed product assortment, prices, and shipping information. During this time, the cookie-usage manipulation (i.e., the second independent variable) was executed. For the cookie-used condition, 30 seconds after participants clicked out of the home page, on their next click, a cookie placement confirmation similar to that found in popular Web browsers appeared as a pop-up window on the screen. It read, "The current Web site wants to set a cookie" and provided details on the name (4544ad01), content (a long series of numbers), domain (.4544adnet4544.com), and expiration (January 17, 2038, 7:00:00 P.M.), and it had buttons that allowed the user to "allow" or "deny" the cookie. Either choice allowed the user to continue examining the Web site. (For both Studies 2 and 3, more than 95% of those receiving the alert accepted the cookie before continuing, possibly because the online task was being conducted on an anonymous computer from the perspective of each respondent.) The cookie-not-used condition had no such pop-up. Note that the detection of the cookie is critical to this study. Because cookies are often a covert marketing tactic, their undetected usage would reasonably be presumed to have no effect on consumer trust or intended behavior. In addition, the likelihood of online users being alerted to cookie placement would normally be relatively low unless the users adjusted their Web browser settings accordingly.

After participants exited from the browser window, they were asked to complete the dependent measures (all of which were seven-point items anchored by "strongly disagree" and "strongly agree") and two demographic items (gender and age). The first dependent measure was a four-item trust scale; items were adapted from the work of Sirdeshmukh, Singh, and Sabol (2002) and Garbarino and Lee (2003) in an attempt to capture both benevolence and competence components of trust. Items stated that the Web site organization "has practices that indicate respect for you as a customer," "has practices that show it values you as a customer," "has practices that favor you as a customer," and "can be relied on to be honest." This was followed by an item that assessed intended patronage ("I would register with this Web site to gain information or products I desire") and one that assessed positive word of mouth ("I would recommend this Web site to friends if they desired the same information or products"). The entire experiment took less than ten minutes to complete.

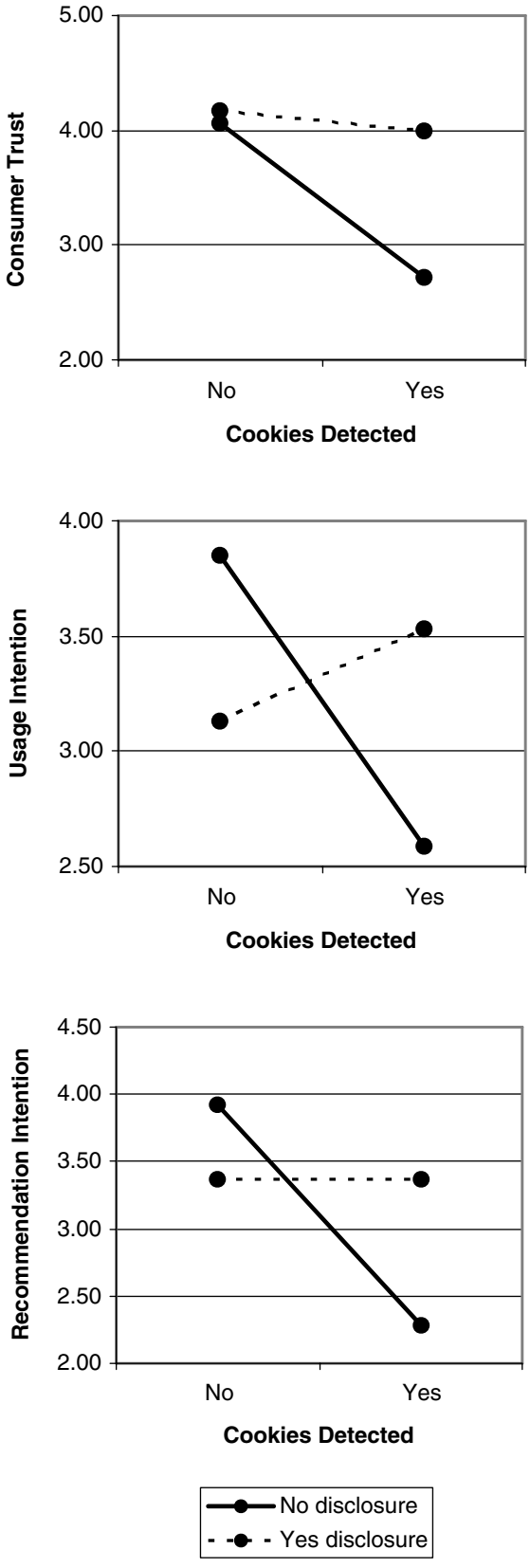
Study 2 Results

Of 217 people initially approached, 154 agreed to participate, for a response rate of 71%. The average age was 36.7 years, and the sample was 61% female. The analyses (unless otherwise indicated) used a 2 (cookie disclosure) × 2 (cookie usage) analysis of variance (ANOVA) design. Initial analyses were conducted to verify that demographic variables and a priori perceived risk levels did not differ across the experimental cells; no such differences were found (all $Fs < .5$).

The hypothesis tests were favorable as well; the results showed support for the hypothesized interaction between cookie usage and cookie disclosure for (1) consumer trust ($F = 7.69$, $p < .01$, $\eta = .22$), (2) usage intention ($F = 9.19$, $p < .01$, $\eta = .24$), and (3) intended recommendations ($F = 10.06$, $p < .01$, $\eta = .25$). In each case, when cookie disclosure was present, there were no effects for cookie usage (all $Fs < 1$). However, when cookie disclosure was not present, cookie usage (versus no usage) led to lower consumer trust ($F = 22.41$, $p < .01$), higher usage intentions ($F = 11.67$, $p < .01$), and higher intended recommendations ($F = 23.11$, $p < .01$). Figure 1 illustrates these results, and means appear in Table 3.

Study 2 demonstrates how consumers' negative reactions to the Web site's cookie usage are attenuated by the Web site organization's a priori explicit disclosure of such usage. In essence, the framework for the social contract was guided by the organization's disclosure that cookies would be used and how they might be useful to the consumer's use

Figure 1. Study 1 Results: Cookie Disclosure Versus Usage Effects



of the Web site. In the case of no disclosure, however, the implied social contract appeared to have been breached, which resulted in lower trust and usage-related intentions.

Study 3: Additional Moderators of Cookie-Usage Effects

Although Study 2 demonstrates the benefit of a priori disclosure, previous work examining consumer reaction to privacy policies has shown that many consumers are either unlikely to read privacy policies or unlikely to comprehend them (Cranor, Guduru, and Arjula 2006; Milne and Culnan 2004; Milne, Culnan, and Greene 2006). Thus, even when a Web site discloses cookie usage, a significant number of online users will not have read or understood such disclosure, suggesting the need to understand which other moderators might influence the negative impact of the detection of cookie usage.

One such moderator could be related to the relative experience of a consumer in interacting with the online environment. As mentioned previously, cookie placement is a relatively ubiquitous practice. As such, Web users with significant online experience would be expected to be more cognizant of the prevalence of cookie use by various online entities than Web users with relatively low amounts of online experience. Those who understand the high degree to which cookies are used should be more likely to expect cookie use for a given Web site and thus should be less affected by the detection of cookie usage by a Web site. Thus:

> H_2: Online experience and consumer detection of a covert identification practice (i.e., an attempt to place a cookie) interact such that when experience is relatively low, consumer detection negatively affects (a) consumer trust, (b) usage intentions, and (c) user recommendations; however, when online experience is relatively high, such effects are attenuated or eliminated.

Another moderator of the impact of cookie use on consumer trust and behavioral intentions would likely be related to consumer perceptions regarding privacy. Prior research has found that consumers often fall into distinct categories regarding their concerns about privacy, with low percentages feeling either alarmed or unconcerned and the majority being somewhat pragmatic in that their privacy concerns are situationally determined (Sheehan 2002). Privacy concerns can lead to lower consumer trust (Jutla and Bodorik 2005), lower willingness to disclose information (Sheehan and Hoy 1999), and lower patronage intentions (Jutla and Bodorik 2005).

However, privacy concerns or beliefs may not reflect a consumer's desire for privacy. Indeed, a group of consumers may have certain privacy beliefs about a particular Web site or technology but vary widely in their desire for privacy. This is not unlike the distinction made between locus of control, in which consumers believe that they have control over an event, and desire for control, in which consumers are motivated to have control over the event (Sprott, Brumbaugh, and Miyazaki 2001). Although locus of control and desire for control have been shown to be separate entities that can influence consumer attitudes and behavior and have been studied from a public policy perspective

Table 3. Mean Results for Studies 2 and 3

	DV: Consumer Trust			DV: Usage Intention			DV: Recommendation		
	Cookie Detected			Cookie Detected			Cookie Detected		
	No	Yes	F-Statistic	No	Yes	F-Statistic	No	Yes	F-Statistic
Study 2									
No disclosure	4.06	2.72	22.41*	3.85	2.59	11.67*	3.92	2.28	23.11*
Yes disclosure	4.17	3.99	.36	3.13	3.53	.96	3.37	3.37	.00
Interaction (disclosure versus cookie detection)			7.69*			9.19*			10.06*
Study 3									
Low online experience	4.76	3.51	26.3*	3.56	2.67	9.11*	3.87	2.68	15.70*
High online experience	4.43	3.99	5.73**	3.90	3.42	4.06**	3.76	3.48	1.27
Interaction (online experience versus cookie detection)			7.29*			1.10			5.63**
Study 3									
Low desire for privacy	5.00	4.57	5.94**	4.20	3.95	1.12	4.29	4.04	1.04
High desire for privacy	4.13	3.07	28.55*	3.30	2.36	13.37*	3.33	2.38	14.32*
Interaction (desire for privacy versus cookie detection)			5.87**			3.86**			3.99**

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

(Miyazaki, Brumbaugh, and Sprott 2001), desire for privacy has received less attention. Indeed, although most privacy-related studies have examined privacy risk (e.g., Miyazaki and Fernandez 2001), concern for privacy (e.g., Phelps, Nowak, and Ferrell 2000), or privacy sensitivity (e.g., Awad and Krishnan 2006), actual desire for privacy is often overlooked or merely included as part of these constructs. However, Phelps, Nowak, and Ferrell (2000) measure "desire for information control" and find that the majority of consumers have some degree of that desire. Nevertheless, they stop short of examining how this desire might affect attitudes or behavioral intentions.

To examine desire for privacy, Sheehan and Hoy's (2000) investigation of the dimensions of online consumer privacy concern is useful. Sheehan and Hoy find three factors of privacy concerns—control over the collection and usage of information, exchange of something of value for requested information, and the potential presence of an established relationship between the online consumer and the Web site organization. With these factors as the basis for privacy concerns, desire for privacy is viewed as a set of desires that include wanting information control, a fair exchange for any information the consumer provides, and a wish to refrain from providing information if no relationship has been formed with the requesting organization.

Prior research has shown that the level of privacy-related concerns or risk can moderate the impact of risk-related factors on trust. For example, Pan and Zinkhan (2006) show that under high-risk conditions, the presence of a privacy policy enhances trust. However, under low-risk conditions, the privacy policy has no such effects. A similar effect can be proposed for the moderating role of desire for privacy on how cookie usage influences attitudes and intentions. Thus, considering that consumers who are relatively low in desire for privacy would presumably be relatively unaffected by privacy-related practices, it follows that desire for privacy could have a moderating effect on the cookie-usage effects discussed previously. Specifically, as desire for privacy increases, so would the effect of cookie usage (or cookie-usage detection) on consumer trust and behavioral intentions. Thus:

H_3: Desire for privacy and consumer detection of a covert identification practice (i.e., an attempt to place a cookie) interact such that when desire for privacy is relatively high, consumer detection negatively affects (a) consumer trust, (b) usage intentions, and (c) user recommendations; however, when desire for privacy is relatively low, such effects are attenuated or eliminated.

Study 3 Methods

Study 3 also used a between-subjects experimental design, manipulating consumer detection of the cookie use by the Web site, as in Study 2. The experimental setting was similar to Study 2 as well, involving the evaluation of the faux Web site of a local school-uniform firm. Participants were adults recruited from a county fair serving a large metropolitan area (with a population of more than 2 million) and were screened to ensure that each had at least one child in a local public or private school that required school uniforms and had made at least one purchase online within the prior 12 months. Incentives were identical to Study 2.

As with Study 2, each participant was asked to sit at a laptop computer and fill out a short questionnaire before conducting the Web site evaluation. This questionnaire had 20 items, 5 of which were used to measure desire for privacy. Most of the other items served as filler to distract participants from the focus on desire for privacy and included questions about general shopping behavior. Several items were also included to validate that the screening was suc-

cessful. The remainder of the procedure continued as in Study 2 and included the cookie manipulation and the same dependent measures, with the addition of a measure that evaluated the duration in years of each consumer's online experience. Online experience was measured as duration (number of years) rather than intensity (number of hours per week) to capture both longitudinal effects of cumulative interaction with the online environment and the effects of cumulative reactions to online-related information (e.g., news reports, discussions with other online users).

The desire-for-privacy measure consisted of five items. The first three assessed desire for control over the collection and usage of information ("It is important for me to know if an organization is trying to collect my personal information," "It is important for me to know what personal information about me an organization has," and "It is important for me to know what an organization will do with my personal information"). It also included one item each that indicated a desire for privacy even in consideration of a fair exchange ("I typically will not provide my personal information to an organization, even if it gives me something of value in exchange for that information") or an ongoing relationship ("I typically will not provide my personal information to an organization, even if we currently have an ongoing business relationship"). The items, which were based on Sheehan and Hoy's (2000) work, were averaged to determine overall desire for privacy.

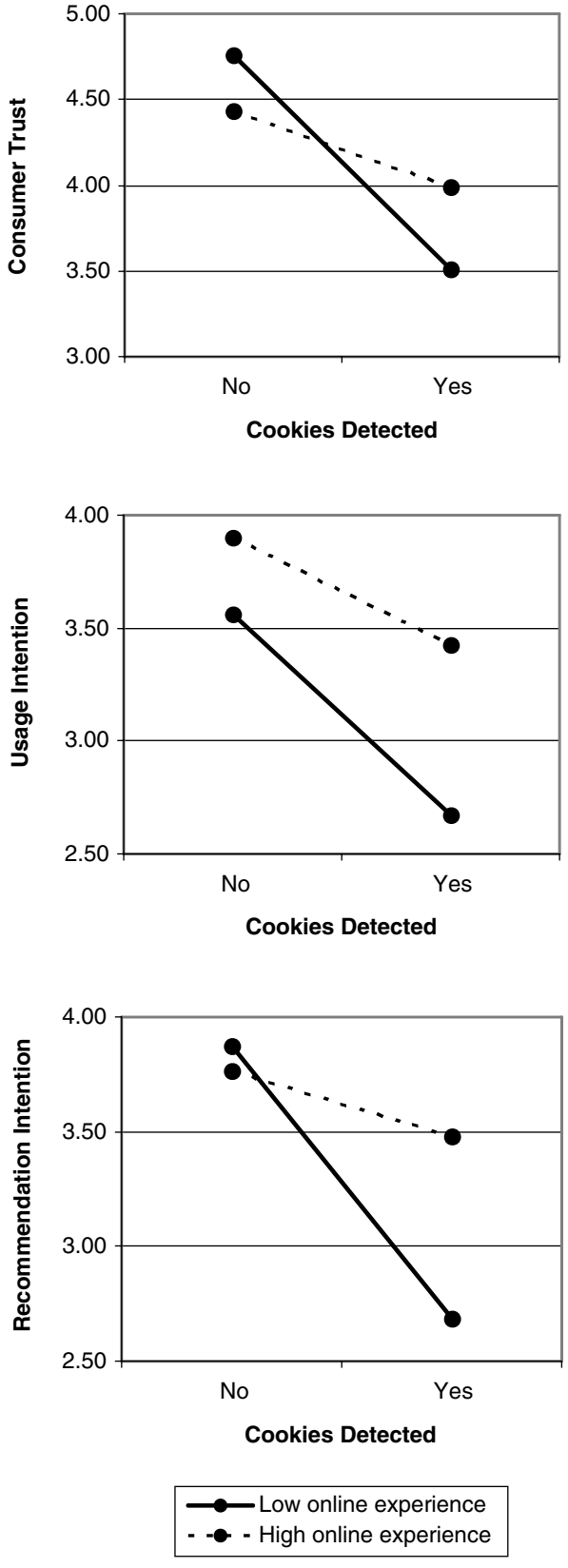
Study 3 Results

Of 544 people approached, 441 (81%) accepted initial screening, and 337 were eligible to participate (for a final response rate of 62%). Participants consisted of 59.6% females, and the average age was 33.2 years. Initial analyses showed that demographics, online experience, and desire for privacy ($\alpha = .93$) did not differ across the cookie-usage conditions. Desire for privacy was not correlated with the number of years of online experience.

H_2 proposed that a consumer's online experience would moderate the effects of cookie usage, such that more online experience would make detection of cookie placement less of a surprise and, thus, less of an influence on attitudes and behavior. To test this, the number-of-years-of-online-experience variable was split into participants with two years or less of time online (n = 132) and those with more than two years online (n = 202). A 2 × 2 ANOVA model showed a significant interaction for consumer trust ($F = 7.29$, $p < .01$, $\eta = .15$), in support of H_{2a}. Specifically, when consumer online experience was low, detection of an online cookie led to lower consumer trust, but when online experience was high, this effect was attenuated. For behavioral intentions, there was the expected, significant interaction for the intended recommendation ($F = 5.63$, $p < .05$, $\eta = .13$) but not for usage intentions ($F = 1.10$, $p = .30$), offering support for H_{2c} but not for H_{2b} (for illustrations, see Figure 2; for means, see Table 3).

H_3 posited an interaction between consumers' desire for privacy and the detection of cookie usage, such that a high desire for privacy would exacerbate any cookie-usage effects. To test this, the desire-for-privacy moderator variable was median split (high desire for privacy: n=168; low desire for privacy: n = 169) and used in 2 × 2 ANOVA models. The hypothesis tests were favorable; the results

Figure 2. Study 2 (H_2) Results: Experience and Cookie-Usage Effects



show the desired interaction between desire for privacy and detection of cookie usage for (1) consumer trust ($F = 5.87$, $p < .05$, $\eta = .13$), (2) usage intention ($F = 3.86$, $p = .05$, $\eta = .11$), and (3) intended recommendations ($F = 3.99$, $p < .05$, $\eta = .11$) (for illustrations, see Figure 3; for means, see Table 3).

General Discussion

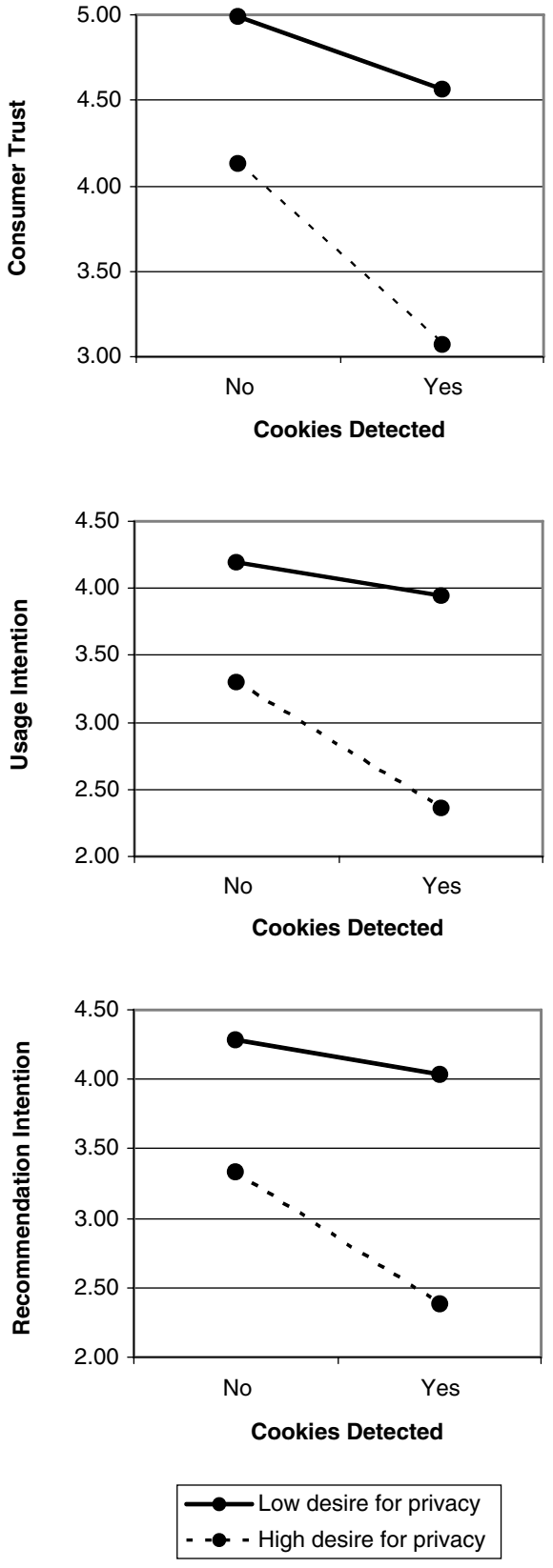
The findings from the three studies provide insights into not only how the state of cookie practice and disclosure has changed since the FTC (2000) recommendation of fair information practices but also how various types of online consumers are likely to react to cookie usage with and without clear disclosure. Specifically, Study 1 found that cookie use—particularly, third-party cookie use—has increased from 2000 to 2007 for the original set of top Web sites. Although this may be viewed as bad news from a consumer privacy perspective, the good news is that disclosure of cookie usage (with a fairly strict definition of disclosure) for Web sites using cookies increased significantly as well. Unfortunately, levels of disclosure are still deficient, particularly for third-party cookies; many Web site managers may believe that mentioning any cookie use is sufficient, despite consumer and policy maker concern over the third-party type. Study 1 also found that the average number of cookies on home pages (for Web sites that used them) increased as well. Most notable is that the covert use of third-party cookies has not declined over the past seven years.

Studies 2 and 3 examined adult consumers with online purchasing experience and found that the detection of cookie use contributes to a decrease in consumer trust with respect to the Web site and a decrease in the behavioral intentions of intended patronage and positive word of mouth. Study 2 showed that this effect is attenuated by the use of a clear a priori disclosure. Study 3 found that the cookie-usage effect is lower for consumers with a longer duration of online experience and for those with a relatively low desire for privacy.

Implications for Online Organizations, Consumers, and Policy Makers

The findings herein and elsewhere that consumers are concerned about their privacy with respect to nonconsensual data collection constitute a serious concern for Web site organizations. This is particularly true considering the evidence that higher levels of privacy concerns lead to lower consumer trust (Jutla and Bodorik 2005), lower willingness to disclose information (Sheehan and Hoy 1999), and lower patronage intentions (Jutla and Bodorik 2005). Study 2 showed that a priori disclosure reduced the effects of cookie usage, suggesting that it is in the best interests of Web site organizations to offer disclosures of cookie use that are prominent enough to be noticed by online consumers. Study 2's cookie disclosure was prominent, fairly simple, relatively short, and relatively easy to read. Milne, Culnan, and Greene's (2006) findings that top-ranked Web site privacy policies averaged almost 20 times longer than the one presented here suggest that it is less likely that consumers will attend to, process, understand, and recall cookie disclosures in the current online environment. Furthermore, findings

Figure 3. Study 2 (H_3) Results: Desire for Privacy and Cookie-Usage Effects



that consumers often do not read privacy policies (Milne and Culnan 2004) and that policies are often written at a reading level higher than that of the consuming public (Milne, Culnan, and Greene 2006) suggest that the mere inclusion of a cookie-usage statement in a privacy policy is insufficient to act as an effective disclosure.

Unfortunately, prior work has shown that consumers are fairly uninformed with respect to cookie use and function (Ha et al. 2006; Hoofnagle 2005; Jensen, Potts, and Jensen 2005; Lavin 2006) and have low usage rates of privacy-related technology (Ha et al. 2006; Jensen, Potts, and Jensen 2005), reducing the likelihood that consumers will discover cookie use. Recent reports suggest that cookies are deleted now more than previously (Regan 2005), but these reports may be questionable in light of research showing large discrepancies between Internet user reports and their actual behavior (Jensen, Potts, and Jensen 2005; Milne, Rohm, and Bahl 2004). Moreover, Hoofnagle (2005) notes that consumers' periodic deletion of all cookies results in the deletion of cookies that contain the opt-out preferences the consumers had chosen for particular Web sites. The result is a blank slate that may put consumers at more privacy risk than if they had maintained at least some of the (opt-out) cookies. Granted, selective allowance, rejection, or deletion of cookies is available on a cookie-by-cookie basis, but the heavy reliance of cookies by many Web sites makes this option extremely inconvenient (Linn 2005). Consider, for example, that the Study 1 examination of 2007 Web sites found up to 59 cookies in one home page visit and that approximately 65% of the Web sites had 5 or more cookies on their home page (approximately 32% had 10 or more).

A potential aid in the evaluation of Web site privacy policies may come in the growing adoption of the Platform for Privacy Preferences, or P3P, which involves a machine-readable format for privacy policies (Cranor 2002, 2003). Cranor, Guduru, and Arjula (2006) contend that an easily programmable automated system lets online consumers know whether a particular Web site has a privacy policy that matches their privacy preferences without the need to read through lengthy text. Such a method is most useful for the fair information principles of "notice" and "choice" (Cranor 2003). However, until such a method is widely adopted, it is of limited use.

Study 1 showed that the percentage of Web sites setting third-party cookies increased substantially and that the percentage of covert third-party placements was not reduced. These findings are likely to add to the growing policy focus on third-party cookies—for example, the FTC (2000) measured only third-party cookie use—which may spawn tactics to circumvent the rejection or deletion of third-party cookies. Indeed, Jackson and colleagues (2006) discuss how cooperation between sites can allow the same or greater levels of privacy invasion, regardless of the level of third-party cookie blocking. For example, data acquired through the placement of original domain cookies can easily and automatically be shared, just as bricks-and-mortar companies have pooled resources in third-party databases for years.

This and other factors (e.g., the recent Supreme Court ruling criticizing the Child Online Protection Act [*Ashcroft v. American Civil Liberties Union* 2004]) have consumer advocates calling for new legislation, though few have offered specifics as to what type of regulations may work on a national and international basis. Some have argued that the European Union can serve as a more effective model of privacy protection (e.g., Strauss and Rogerson 2002). Indeed, Jamal, Maier, and Sunder (2005) find that general cookie use and third-party cookie use were lower and that cookie disclosure for third-party cookies was higher for U.K. Web sites (under the European Union privacy laws) than for U.S. sites. However, they also find that the United States fared much better with other types of disclosure practices (e.g., the presence of a privacy policy, its ease of access, and how information is used).

These various issues and concerns suggest several recommendations for public policy makers. First, disclosure of cookie use must be clearly noticeable and understandable by the consuming public (regardless of age or level of online expertise). Second, future Web browsers should be designed to have the option of deleting categories of cookies so that opt-out (or opt-in) preferences are not deleted at the same time as other cookie deletions. Third, policy makers should note that even the complete elimination of third-party cookie use by Web sites can be circumvented by cooperative strategies with third parties in which information is transferred after the Web site's use of original domain cookies. Finally, Web site organizations should be informed that it is to their advantage to disclose cookie use in order to develop higher levels of trust and patronage intentions with their online users, particularly as the detection of cookie use becomes less cumbersome for these users.

Further Research

The issues involved in securing an acceptable degree of Internet privacy are diverse. As such, there are several research opportunities. Recent efforts by scholars to understand actual consumer behavior with respect to privacy practices (e.g., Jensen, Potts, and Jensen 2005; Milne and Culnan 2004) and content analyses of privacy policies (Milne, Culnan, and Greene 2006; Schwaig, Kane, and Storey 2005) can merge to create better methods of disclosure, which should lead to greater choice, access, and security (see FTC 2000). The findings that disclosure can have positive effects on consumer reaction to cookie detection support these efforts. However, there is a greater need to examine consumer response to these practices, particularly in light of potentially changing consumer attitudes toward privacy. Awad and Krishnan (2006) note that consumers who desire more information transparency are less willing to provide information that will allow them the personalization they seek. Future investigations into consumers' desire for privacy (shown in Study 3 to moderate reactions to cookie detection) and its potential changes over time should aid in understanding how disclosure may or may not affect consumer reactions to privacy invasions as the Internet matures. Furthermore, Studies 2 and 3 focused on parents who evaluated a Web site that sold children's school uniforms. As such, the respondents may have been overly sensitive to privacy issues. This limitation should be remedied with future work that examines adults' reactions to other

types of Web sites, as well as children's reactions to child-oriented Web sites (see, e.g., Lwin, Stanaland, and Miyazaki 2008).

Study 2 presented a simple disclosure of cookie use. There is currently much diversity in how Web sites present essentially the same disclosure information. For example, cookies are described in privacy policies as "the industry standard," "common to most popular Web sites," and "part of everyday surfing of the Internet." Their myths regarding the ability to "access information from other portions of the hard drive" or "run programs on the computer" are commonly debunked. They are promoted as "helpful" and/or "necessary" for navigating Web sites and conducting online transactions. However, few Web sites appear to be making clear an exchange-of-benefits approach in which the acceptance of cookies is paired with meaningful compensation (Goodwin 1991; Milne and Gordon 1993). Indeed, Sheehan and Hoy's (2000) discussion of exchange and relationships may prove valuable in developing privacy policies that serve as both fair information practices and marketable offerings.

Finally, new technologies may make cookie concerns obsolete before their privacy issues have been resolved. The use of Web bugs (clear GIFs) has increased dramatically and offers a way to track not only Web page navigation but also the opening of individual e-mail messages (Bayan 2001; Martin, Wu, and Alsaid 2003; Security Space 2007).

Conclusion

Online privacy continues to be an issue of concern for consumers, online organizations, and policy makers. Nonconsensual identification through the use of original domain and third-party cookies is a particular privacy concern that has caught the attention of both government entities and consumer groups. The current research presents an investigation into not only cookie practice versus disclosure over time but also how online consumers react to the detection of cookie use by a Web site. Although a priori disclosure of cookie usage weakens the negative effects of cookie detection on consumer trust and behavioral intentions, concerns about the current methods of disclosure suggest the need for further examination. The finding that experience and desire for privacy also moderate the effects of cookie usage may suggest alternative methods of addressing an issue that hopefully will be resolved long before the final cookie from Study 1 is scheduled to expire on the research computer's hard drive, that being April 8, 2075 (cookie set by sonyonline.com).

References

Antón, Annie I., Qingfeng He, and David L. Baumer (2004), "Inside JetBlue's Privacy Policy Violations," *IEEE Security & Privacy*, 2 (November–December), 12–18.

Ashcroft v. American Civil Liberties Union (2004), No. 03-218, 542 U.S. 656, 322 F.3d 240, affirmed and remanded.

Awad, Neveen Farag and M.S. Krishnan (2006), "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly*, 30 (March), 13–28.

Bayan, Ruby (2001), "Privacy Means Knowing Your Cookies," *Link-Up*, 18 (January–February), 22–23.

Berghel, Hal (2002), "Hijacking the Web," *Communications of the ACM*, 45 (April), 23–27.

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

Chapman, Scott and Gurpreet Dhillon (2002), "Privacy and the Internet: The Case of DoubleClick, Inc.," in *Social Responsibility in the Information Age: Issues and Controversies*, Gurpreet Dhillon, ed. Hershey, PA: Idea Group Publishing, 75–88.

Chellappa, Ramnath K. and Raymond G. Sin (2005), "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, 6 (April), 181–202.

Cranor, Lorrie Faith (1999), "Internet Privacy," *Communications of the ACM*, 42 (February), 29–31.

——— (2002), *Web Privacy with P3P*. Cambridge, MA: O'Reilly & Associates.

——— (2003), "P3P: Making Privacy Policies More Useful," *IEEE Security & Privacy*, 1 (November–December), 50–55.

———, Praveen Guduru, and Manjula Arjula (2006), "User Interfaces for Privacy Agents," *ACM Transactions on Computer-Human Interaction*, 13 (June), 135–78.

Culnan, Mary J. (1995), "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketers," *Journal of Direct Marketing*, 9 (Spring), 10–19.

Department of Transportation (2003), "Report on Privacy Concerns for Web Visitors," Report No. FI-2001-006, (November 3), (accessed March 24, 2007), [available at http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/fi2001006.pdf].

Dixon, Pam and Beth Givens (2004), "Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail," (April 19), (accessed March 24, 2007), [available at http://www.privacyrights.org/ar/GmailLetter.htm].

Dunfee, Thomas W., N. Craig Smith, and William T. Ross Jr. (1999), "Social Contracts and Marketing Ethics," *Journal of Marketing*, 63 (July), 14–32.

FTC (2000), "Privacy Online: Fair Information Practices in the Electronic Marketplace," report to Congress, (May 2000), (accessed March 24, 2007), [available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf].

——— (2007), "Chairman Announces Appointments in the Bureau of Consumer Protection," press release, (January 29), (accessed February 21, 2007), [available at http://www.ftc.gov/opa/2007/01/fyi0713.htm].

Garbarino, Ellen and Olivia F. Lee (2003), "Dynamic Pricing in Internet Retail: Effects on Consumer Trust," *Psychology & Marketing*, 20 (June), 495–513.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 19 (Spring), 149–66.

Gralla, Preston (2007), "How to Surf Anonymously Without a Trace," *Computerworld*, (March 12), (accessed March 24, 2007), [available at http://www.computerworld.com].

Ha, Vicki, Farah Al Shaar, Kori Inkpen, and Lina Hdeib (2006), "An Examination of User Perception and Misconception of Internet Cookies," in *CHI 2006 Extended Abstracts on Human Factors in Computing Systems*. Montréal: Association for Computer Machinery, 833–38.

Hemphill, Thomas A. (2000), "DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned," *Business and Society Review*, 105 (Fall), 361–72.

Hoofnagle, Chris Jay (2005), "Privacy Self Regulation: A Decade of Disappointment," Electronic Privacy Information Center, (accessed March 24, 2007), [available at http://www.epic.org/reports/decadedisappoint.pdf].

Hoy, Mariea Grubbs and Joseph Phelps (2003), "Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern," *Journal of Public Policy & Marketing*, 22 (Spring), 58–70.

Jackson, Collin, Andrew Bortz, Dan Boneh, and John C. Mitchell (2006), "Protecting Browser State from Web Privacy Attacks," in *Proceedings of the 15th International Conference on World Wide Web*. New York: Association for Computer Machinery, 737–44.

Jamal, Karim, Michael Maier, and Shyam Sunder (2003), "Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market," *Journal of Accounting Research*, 41 (May), 285–309.

———, ———, and ——— (2005), "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom," *Journal of Accounting Research*, 43 (March), 73–96.

Jarvenpaa, Sirrka L., Noam Tractinsky, and Michael Vitale (2000), "Consumer Trust in an Internet Store," *Information Technology and Management*, 1 (November), 45–71.

Jensen, Carlos, Colin Potts, and Christian Jensen (2005), "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies*, 63 (July), 203–227.

Jutla, Dawn N. and Peter Bodorik (2005), "Sociotechnical Architecture for Online Privacy," *IEEE Security & Privacy*, 3 (March–April), 29–39.

King, Carol (2001), "Privacy Advocate Calls on Congress to Act," *InternetNews*, (March 29), (accessed March 24, 2007), [available at http://www.internetnews.com/ec-news/article.php/4_728911].

Lavin, Marilyn (2006), "Cookies: What Do Consumers Know and What Can They Learn?" *Journal of Targeting, Measurement and Analysis for Marketing*, 14 (July), 279–88.

Lederer, Scott, Jason I. Hong, Anind K. Dey, and James A. Landay (2004), "Personal Privacy Through Understanding and Action: Five Pitfalls for Designers," *Personal and Ubiquitous Computing*, 8 (November), 440–54.

Leibrock, Larry R. (1997), "Privacy, Surveillance, and Cookies," in *Electronic Marketing and the Consumer*, Robert A. Peterson, ed. Thousand Oaks, CA: Sage Publications, 155–62.

Linn, John (2005), "Technology and Web User Data Privacy," *IEEE Security & Privacy*, 3 (January–February), 52–58.

Lwin, May O., Andrea J.S. Stanaland, and Anthony D. Miyazaki (2008), "Protecting Children's Privacy Online: How Parental Mediation Strategies Affect Website Safeguard Effectiveness," *Journal of Retailing*, forthcoming.

Martin, David, Hailin Wu, and Adil Alsaid (2003), "Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use," *Communications of the ACM*, 46 (December), 258–64.

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar (2002), "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research*, 13 (September), 334–59.

Millett, Lynette I., Batya Friedman, and Edward Felten (2001), "Cookies and Web Browser Design: Toward Realizing Informed Consent Online," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: Association for Computer Machinery, 46–52.

Milne, George R. (2000), "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," *Journal of Public Policy & Marketing*, 19 (Spring), 1–6.

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

——— and Mary J. Culnan (2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing*, 18 (Summer), 15–29.

———, ———, and Henry Greene (2006), "A Longitudinal Assessment of Online Privacy Notice Readability," *Journal of Public Policy & Marketing*, 25 (Fall), 238–49.

——— and Mary Ellen Gordon (1993), "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy & Marketing*, 12 (Fall), 206–213.

———, Andrew J. Rohm, and Shalini Bahl (2004), "Consumers' Protection of Online Privacy and Identity," *Journal of Consumer Affairs*, 38 (Winter), 217–32.

Miyazaki, Anthony D., Anne M. Brumbaugh, and David E. Sprott (2001), "Promoting and Countering Consumer Misconceptions of Random Events: The Case of Perceived Control and State-Sponsored Lotteries," *Journal of Public Policy & Marketing*, 20 (Fall), 254–67.

——— 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 (Spring), 27–44.

Moorman, Christine, Rohit Deshpandé, and Gerald Zaltman (1993), "Factors Affecting Trust in Market Research Relationships," *Journal of Marketing*, 57 (January), 81–101.

Morgan, Robert M. and Shelby D. Hunt (1994), "The Commitment–Trust Theory of Relationship Marketing," *Journal of Marketing*, 58 (July), 20–38.

Palmer, Maija (2007), "Google Bows to Privacy Concerns on Search Data," *Financial Times*, (March 15), (accessed March 24, 2007), [available at http://www.msnbc.msn.com/id/17618203/].

Pan, Yue and George M. Zinkhan (2006), "Exploring the Impact of Online Privacy Disclosures on Consumer Trust," *Journal of Retailing*, 82 (4), 331–38.

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

Raghu, T.S., P.K. Kannan, H.R. Rao, and A.B. Whinston (2001), "Dynamic Profiling of Consumers for Customized Offerings over the Internet: A Model and Analysis," *Decision Support Systems*, 32 (December), 117–34.

Reagle, Joseph and Lorrie Faith Cranor (1999), "The Platform for Privacy Preferences," *Communications of the ACM*, 42 (February), 48–51.

Regan, Keith (2005), "Web Analytics Industry Confronts Cookie-Deletion Trend," *E-Commerce Times*, (May 25), (accessed March 24, 2007), [available at http://www.ecommercetimes.com].

Schwaig, Kathy Stewart, Gerald C. Kane, and Veda C. Storey (2005), "Privacy, Fair Information Practices and the Fortune 500: The Virtual Reality of Compliance," *ACM SIGMIS Database*, 36 (Winter), 49–63.

Security Space (2007), "Web Bug Report," (March 1), (accessed March 24, 2007), [available at http://www.securityspace.com/s_survey/data/man.200702/webbug.html].

Sheehan, Kim Bartel (2002), "Toward a Typology of Internet Users and Online Privacy Concerns," *The Information Society*, 18 (January), 21–32.

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

——— and Mariea Grubbs Hoy (1999), "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," *Journal of Advertising*, 28 (Fall), 37–51.

——— and ——— (2000), "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, 19 (Spring), 62–73.

Sirdeshmukh, Deepak, Jagdip Singh, and Barry Sabol (2002), "Consumer Trust, Value, and Loyalty in Relational Exchanges," *Journal of Marketing*, 66 (January), 15–37.

Sit, Emil and Kevin Fu (2001), "Web Cookies: Not Just a Privacy Risk," *Communications of the ACM*, 44 (September), 120.

Sprott, David E., Anne M. Brumbaugh, and Anthony D. Miyazaki (2001), "Motivation and Ability as Predictors of Play Behavior in State-Sponsored Lotteries: An Empirical Assessment of Psychological Control," *Psychology & Marketing*, 18 (September), 973–83.

Strauss, Jared and Kenneth S. Rogerson (2002), "Policies for Online Privacy in the United States and the European Union," *Telematics and Informatics*, 19 (May), 173–92.

United States Courts (2000), "Internet and Electronic Case Filing Raise Privacy Concerns," *The Third Branch*, 32 (June), Administrative Office of the United States Courts, (accessed March 24, 2007), [available at http://www.uscourts.gov/ttb/june00ttb/internet.html].