

This article was downloaded by: [University of Arizona]

On: 5 August 2009

Access details: Access Details: [subscription number 789363144]

Publisher Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Health Communication

Publication details, including instructions for authors and subscription information:

<http://www.informaworld.com/smpp/title-content=t775653649>

Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements

Stephen A. Rains^a; Leslie A. Bosch^b

^a Department of Communication, University of Arizona, ^b The Division of Family Studies and Human Development, University of Arizona,

Online Publication Date: 01 July 2009

To cite this Article Rains, Stephen A. and Bosch, Leslie A. (2009) 'Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements', *Health Communication*, 24:5, 435 — 446

To link to this Article: DOI: 10.1080/10410230903023485

URL: <http://dx.doi.org/10.1080/10410230903023485>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Privacy and Health in the Information Age: A Content Analysis of Health Web Site Privacy Policy Statements

Stephen A. Rains

*Department of Communication
University of Arizona*

Leslie A. Bosch

*The Division of Family Studies and Human Development
University of Arizona*

This article reports a content analysis of the privacy policy statements (PPSs) from 97 general reference health Web sites that was conducted to examine the ways in which visitors' privacy is constructed by health organizations. PPSs are formal documents created by the Web site owner to describe how information regarding site visitors and their behavior is collected and used. The results show that over 80% of the PPSs in the sample indicated automatically collecting or requesting that visitors voluntarily provide information about themselves, and only 3% met all five of the Federal Trade Commission's Fair Information Practices guidelines. Additionally, the results suggest that the manner in which PPSs are framed and the use of justifications for collecting information are tropes used by health organizations to foster a secondary exchange of visitors' personal information for access to Web site content.

The emergence of the Internet and World Wide Web as important resources for health information, care, and services has been met with both enthusiasm and trepidation among scholars and practitioners (Cline & Haynes, 2001; Gurak & Hudson, 2006; Turner, 2003). One central area of concern involves the privacy of individuals using the Web for health purposes. Instances when consumers are asked to voluntarily enter detailed information about themselves or their health condition, as well as those situations when data about consumers' information-seeking behavior is tracked automatically, present serious privacy concerns (LaRose & Rifon, 2006; Markel, 2005; Mundy, 2006; Westin, 1967). Further, increased information sharing among health providers, pharmacies, and insurance agencies, which has been greatly facilitated by the Internet, has rendered individuals' personal information susceptible to misuse and privacy violations ranging from selling patient records to using medical records as a basis for employment decisions (Baumer, Earp, & Payton, 2000;

Choy, Hudson, Pritts, & Goldman, 2001). One such concern was realized during 2001 when a pharmaceutical company inadvertently revealed the e-mail addresses of individuals taking an anti-depressant medication (O'Harrow, 2001).

To address consumers' privacy concerns, health Web sites have in recent years begun posting privacy policy statements (PPSs). These statements are a formal document created by the individual(s) or organization(s) operating the Web site to describe how information regarding site visitors and their behavior is collected and used. To date, health Web site PPSs have received fairly little attention by scholars (e.g., Mundy, 2006; Sheehan, 2005). Yet the large number of individuals using the Web to acquire medical information and care, coupled with concerns about information privacy, make it imperative that scholars and practitioners fully understand these important artifacts of contemporary health communication and their implications for health consumers. In addition to providing detailed information about a Web site's monitoring practices, PPSs offer a window to explore the ways in which privacy is constructed by contemporary health institutions and articulated to Web site visitors. PPSs articulate how health organizations view visitor

Correspondence should be addressed to Stephen A. Rains, Department of Communication, University of Arizona, Tucson, AZ 85721-0025.
E-mail: srains@email.arizona.edu

privacy and how they expect that Web site visitors should view their own privacy (Markel, 2005).

This article reports a content analysis of the PPSs from general-reference health Web sites. These types of health Web sites (e.g., medlineplus.gov, webmd.com) contain information about a variety of health topics and, as such, are a widely-used resource for health-related inquires (Wood, Benson, LaCroix, Siegel, & Fariss, 2005). Exchange theory and, in particular, the notion of a secondary exchange (Culnan & Bies, 2003) are offered as a theoretical foundation for the analysis. In addition to evaluating PPS content, the use of justifications for collecting information and the framing of visitors' interests in privacy are examined as rhetorical strategies used to encourage visitors to disclose personal information in exchange for access to a medical Web site. In the following section, research examining privacy and health on the Web is reviewed to provide a foundation for study hypotheses and research questions.

HEALTH AND PRIVACY ON THE WEB

Background on PPSs

Privacy refers to an "individual's right to control access to his or her personal information within defined contexts" (Markel, 2005, p. 202). A Web site PPS, then, explains how the Web site collects and uses information gathered from or about its visitors (Sheehan, 2005). Web sites gather information in ways that are both visible and transparent to visitors. Sites may ask visitors to voluntarily enter information about themselves (e.g., for purposes of registration or purchasing products), such as their contact, demographic, and financial information, and even information about their health condition(s). Web sites may also automatically collect information about visitors and their behavior—although almost 40% of 1,200 respondents in Turow's (2003) nationally representative survey were not aware that this was the case. One method of collecting information automatically is through the use of "cookies," which are small files stored on the visitor's computer and accessed by the host site (Hong, McLaughlin, Pryor, Beaudoin, & Grabowicz, 2005). Cookies can be used to collect a variety of different types of information without a site visitor's knowledge or consent, including a visitor's computer hardware and software, Internet protocol (IP) address, and Web use behavior such as the frequency, duration, and pages visited on a particular Web site. Use of third-party cookies, in particular, have raised concerns because these cookies originate outside of the Web site being visited and are often used by advertisers to create a profile of one's Web-use behavior on sites sponsored by the advertiser.¹

¹Legislation in the form of the Consumer Online Privacy and Disclosure Act (H.R. 347) was proposed in 2001 to limit user profiling by making it illegal for organizations to use persistent cookies (which remain on one's computer after one has left a Web site) and subsequently creating consumer profiles. This legislation, however, was referred to a subcommittee and has not been further pursued.

Consumer responses to privacy on the Internet have been described as a paradox (LaRose & Rifon, 2007). Research suggests that consumers are concerned with their privacy (Choy et al., 2001; Fallows, 2005; Metzger & Docter, 2003; National Telecommunications and Information Administration, 2000; Westin, 2003). These concerns, however, do not appear to influence Internet use behavior such as revealing detailed personal information (Metzger, 2006) or the use of privacy seals (Rifon, LaRose, & Choi, 2005)—although there are exceptions (e.g., Milne & Culnan, 2004). One reason for this apparent paradox is consumer misunderstanding of Web site data-collection procedures and PPSs (Turow, 2003). Turow and Hoofnagle (2006) argue that consumers perceive PPSs and the phrase "privacy policy" as an indication that their personal information will be protected; consumers do not recognize that PPSs simply describe the organization's data-collection and sharing practices. Further, those individuals who do venture to read a Web site's PPS are often met with a document that is replete with legalese and difficult to comprehend (Milne & Culnan, 2004). Indeed, Milne, Culnan, and Greene's (2006) research indicates that PPSs from popular Web sites require an 11th to 12th grade education to understand and have become significantly more complex over time.

Various procedures have been established to help govern the collection and release of personal health information. The Department of Health and Human Services (2000) developed the "Privacy Rule" as an outgrowth of the 1996 Health Information Portability and Accountability Act. Yet because a majority of health Web sites are not operated by organizations (such as insurers) that are covered by the Privacy Rule, they do not fall under the purview of the Rule (Choy et al., 2001; Goldman & Hudson, 2000). Health Web sites are, however, subject to the Fair Information Principles established by the Federal Trade Commission (FTC; Choy et al., 2001). The FTC contends that organizations operating a Web site have a responsibility to implement procedures that protect information that is personally identifiable. The FTC established five guidelines to support industry self-regulation of privacy practices, including the principles of notice, choice, access, security, and redress. Notice mandates that Web sites identify who is collecting the information and to what uses the data will be put. Choice involves providing site visitors with options regarding how their personal information may be used, particularly in regard to information-sharing with other organizations. Access requires that sites provide visitors with the opportunity to examine the data collected and to contest the accuracy of the data. Security requires sites to ensure that personal information (e.g., credit card numbers) is securely transmitted and stored. Redress requires that there is a due process for users to file complaints to sites and that there are sanctions for noncompliance with the site's policy.

Research conducted to date on Web site privacy polices suggests that, although most have a PPS, relatively few fully comply with the FTC's guidelines (FTC, 2000; Hong

et al., 2005; LaRose & Rifon, 2006; Ryker, Lafleur, Cox, & McManis, 2002). In regard to health Web sites in particular, Mundy (2006) examined a sample of medical Web sites in the United Kingdom, reporting that only 61% listed a privacy policy. Of those sites, most met the notice and choice guidelines but were lacking in regard to the remaining three guidelines. In addition, Sheehan (2005) conducted an analysis of direct-to-consumer Web sites for pharmaceuticals and found that most sites in the sample included information to meet the notice guideline; however, a third or fewer of the sites complied with the remaining guidelines.

Secondary Exchange, Privacy, and Health Web Site PPSs

Social exchange theory (Thibault & Kelley, 1959) and exchange theory (Bagozzi, 1975; Houston & Gassenheimer, 1987) provide a useful theoretical framework in which to ground an analysis of the way that consumers' privacy is constructed in Web site PPSs. These two theories are rooted in the assumption that individuals weigh the costs and benefits of engaging in a transaction. When the benefits outweigh the costs, individuals are more likely to participate. Trust plays a central role in mitigating the risk associated with the transaction.

Culnan and Bies (2003) explain one particular type of exchange that is especially relevant in the context of privacy and use of the Web for health purposes. A "secondary exchange" occurs when an individual "makes a non-monetary exchange of their personal information for value such as higher quality service or personalized offers or discounts" (p. 326). Personal information forms the currency held by Web users in a secondary exchange. Whether voluntarily disclosed by consumers or automatically collected through the use of cookies, consumers' personal information is bartered for access to and use of a medical Web site. As LaRose and Rifon (2006, p. 1016) note, "website proprietors have an interest in collecting consumer information and that consumer disclosure of personal information is often the currency of exchange to obtain desired outcomes at a website." Although secondary exchanges can result in benefits for Web site visitors—including access to information or services, personalized content, discounts, loyalty program memberships, and so forth (LaRose & Rifon, 2007)—they also raise potential privacy concerns. Individuals must surrender personal information that may range from their age or ethnic background to detailed information about their health, which in turn may be shared with or sold to other organizations. Such disclosures make individuals susceptible to a variety of negative outcomes, such as the misuse of personal medical information (Goldman & Hudson, 2000; Mundy, 2006), fraud (Metzger, 2004), and even fostering a surveillance society (Gandy, 1996).

PPSs play a central role in the secondary exchange (Milne & Culnan, 2004). In addition to detailing the data-collection practices used by the organization operating the

Web site, PPSs construct privacy for Web users. As such, PPSs can be viewed as a persuasive tool used by organizations to shape visitors' perceptions of the risk associated with sharing information and the nature of the secondary exchange (LaRose & Rifon, 2006; Markel, 2005). LaRose and Rifon (2006) succinctly summarize this role of PPSs, arguing that they are a "form of persuasive communication that attempts to minimize the risks of providing personal information while emphasizing the benefits of personal disclosure" (p. 209). PPSs can be used to manage the cost-benefit tension associated with the secondary exchange.

Recent research suggests two strategies used in PPSs to construct visitors' privacy and facilitate the secondary exchange of visitor information for site access. One such feature is the manner in which a PPS is framed.² Markel (2005) argues that organizations may frame the importance of visitor privacy in different ways: A PPS may be explicitly framed as pro-visitor. Organizations may articulate concern for the visitor's privacy (e.g., "Your privacy is important to us."), thus aligning their interests with site visitors' interests. From this perspective, the organization operating the Web site is concerned about visitors' privacy and, presumably, will act in visitors' best interests. In contrast, organizations may recognize that visitors are concerned about their own privacy—though, presumably, the organization is not (e.g., "We know that you're concerned with your privacy"). Markel (2005) explains, "although customers value their privacy, there is an important countervailing value: the necessity or desirability of collecting personal information" (p. 207). The unstated claim in a PPS framed this way is that the visitors' interests in privacy are subordinate to a company's interest in collecting information.

A second strategy for facilitating the secondary exchange is the inclusion of justifications for collecting data about visitors (LaRose & Rifon, 2006; Markel, 2005). Although some justifications may be difficult to follow, the act of including what ostensibly appears to be a rationale may signal to consumers that data are being collected for legitimate purposes. LaRose and Rifon (2006) conducted a content analysis of PPSs and found a positive relationship between the number of arguments in favor of monitoring and the total number of privacy disturbances perpetrated by the Web site. They contend that the arguments in favor of monitoring function to counter any perceived privacy risks among site visitors.

Despite the central role they may play in facilitating the secondary exchange, little is known beyond LaRose and Rifon's (2006) initial work about the relationship between the use of justifications in PPSs and PPS framing and the nature of personal information collected from Web site visitors. The

²To clarify, the use of the term *framing* does not follow from Kahneman & Tversky's (1979) work on framing. Although there may be some overlap, there is a substantial difference in Markel's use of the term *framing* and the loss- and gain-framed messages discussed by Kahneman and Tversky.

preceding research suggests that these two tactics may be used by organizations to mitigate the risks perceived by Web site visitors in regard to divulging personal information. As such, it is plausible that organizations using a pro-consumer framed PPS or one that offers justifications may collect more personal information from site visitors. Because assurances or reasons for collecting information are provided in the PPS, the organization operating the Web site may expect that consumers will be more comfortable sharing information.

Research Questions and Hypotheses

The preceding discussion of PPSs, social exchange, and secondary exchanges raises a number of important questions that, being answered, would inform health communication scholars and practitioners. First, it would be useful to know what types of personal information are collected by general-reference health Web sites. In addition, although previous research suggests that privacy is important to consumers who venture online for health information, care, and services, consumers are left to the self-regulation of health Web sites (based on FTC's Fair Information Practices) to protect their privacy and secure their information. Accordingly, it is important to know more about the information collection practices reported in the PPSs of general-reference health Web sites, including the degree to which they conform to the FTC guidelines. The following research questions were proposed to address these issues:

- RQ1: What types of information are (a) voluntarily and (b) automatically collected from visitors to general-reference health Web sites?
- RQ2: Do the PPSs of general-reference health Web sites conform to the FTC's Fair Information Practice guidelines for PPSs?

In addition to examining the types of information included in PPSs, a second goal of this study was to understand the way in which privacy was constructed in health Web site PPSs. It was argued that PPSs are persuasive documents designed to foster the secondary exchange of personal information for Web site usage. PPSs framed as pro-visitor or offering justifications for collecting information were posited to be more likely to report collecting personal information from Web site visitors. Both of these tropes could serve to mitigate Web site visitors' perceptions of risk and legitimize the secondary exchange. It is less clear, however, if PPSs that are framed as pro-visitor and those offering justification will be more likely to conform to the FTC guidelines. Finally, given previous research demonstrating the low levels of readability associated with PPSs, it would be worthwhile to assess the readability of PPSs from general-reference health Web sites. It seems possible that there may be differences in the readability of PPSs from sites framed

as pro-visitor and those offering justifications as compared to those that are not pro-visitor and that do not offer justifications for monitoring visitors. Increasing the readability of a site's PPS may serve to underscore the pro-visitor framing of the PPS and justifications for monitoring by reinforcing the notion that the Web site is not engaging in any disreputable data-collection practices; yet decreasing the readability of a PPS could obscure a Web site's data collection practices and encourage visitors to rely solely on the pro-visitor framing or inclusion of justifications in weighing their privacy risks. To examine these issues, the following hypotheses and research questions are posed:

- H1: Organizations with a pro-visitor framed PPS will be more likely than those with a PPS not framed as pro-visitor to (a) request and (b) automatically track information from site visitors.
- H2: Organizations with a PPS that includes a justification for collecting personal information will be more likely than those with a PPS that does not include a justification to (a) request and (b) automatically track information from site visitors.
- RQ3: Are there any differences in the degree to which organizations with a pro-visitor-framed PPS conform to FTC guidelines in comparison with those not framed as pro-visitor?
- RQ4: Are there any differences in the degree to which the PPSs from organizations that include a justification for collecting information conform to FTC guidelines compared to those that do not include a justification?
- H3: Differences exist in the readability of PPSs based on (a) whether or not the PPS is framed as pro-visitor and (b) whether or not the PPS includes justifications for monitoring.

METHOD

Sample

The PPSs analyzed in this study were collected from general-reference health Web sites during September, October, and November of 2006. General-reference sites are defined as those Web sites containing information about multiple, distinct health topics. Web sites such as Medline-Plus.gov and WebMD.com, for example, provide information about hundreds of different health topics ranging from acid reflux to Zoster virus. Granted, the plethora of Web sites with health-related content (e.g., Cline & Haynes, 2001, estimated that 70,000 health-related sites exist), sampling general-reference Web sites has two key advantages. First, these types of Web sites provide consumers with a centralized location for information about a multitude of medical issues and, as such, are widely used by information seekers (Wood et al., 2005). Second, because these sites address a variety of medical topics, they are

more likely to be representative of the broader population of health Web site PPSs than Web sites addressing a specific medical concern.

A two-step procedure was used to locate the general-reference health Web sites in the sample. First, the terms *medical information* and *health information* were separately entered into three popular Web search engines (Google, Yahoo, and MSN). The top 100 sites returned from each query were checked to identify general reference sites; a total of 600 sites were examined during this step. This first approach to identify PPSs reflects the general health information-seeking behavior of American adults (i.e., relying on a search engine; Fox, 2006; Fox & Rainie, 2000) and has been used in previous research examine PPSs from health Web sites (Mundy, 2006). Second, approximately 15 Web-based directories for health-related Web sites (e.g., <http://www.health.gov/nhic/pubs/clearinghouses.html>, www.medlist.com, <http://www.allhealthnet.com>) were reviewed to locate additional general-reference sites. The general-reference sites identified during both steps were combined and redundancies were removed.

PPSs from a total of 97 unique general-reference health Web sites were identified and recorded.³ The addresses for all 97 Web sites are presented in Table 1. Forty-six sites had a “.com” top-level domain, 27 had an “.org” domain, 20 were “.gov” sites, and 4 had an “.edu” domain. In terms of the number of different health topics addressed on each Web site, 69.1% of the Web sites in the sample addressed over 100 different health topics. Only one Web site addressed fewer than 10 different health topics: the National Prevention Information Network (www.cdcnpi.org), which is a service of the Centers for Disease Control and Prevention, has information about HIV/AIDS, sexually-transmitted diseases, tuberculosis, and communities at risk. The length of PPSs in the sample ranged from as few as 30 words to 5,952 words ($M = 111.98$, $SD = 1075.65$). Only one of the Web sites in the sample required registration for visitors to access its content, and 34 (35%) of the Web sites included advertisements. Finally, 14 of the general-reference sites ranked in the top 25 most popular health Web sites in the world by the Web monitoring company Alexa during early 2007.⁴

³It should be noted that, although we were able to identify 106 different general-reference Web sites, there were three sets of Web sites (totaling 12 different sites) that were owned by the same companies and had the same PPSs. Only one PPS from each of the three sets of sites was included in the data set, resulting in the sample of 97 different PPSs.

⁴Alexa determines Web site popularity through tracking the Web-use behavior of those individuals who use Alexa’s search engine toolbar over a rolling 3-month period. The rankings produced by the company should be viewed with this in mind. In this context, the Alexa rankings provide some general evidence that sites included in this sample ranged in popularity and included some of the more heavily trafficked health-related Web sites in the world.

Data Analysis

PPSs were content-analyzed to test the hypotheses and answer the research questions. A printed copy of each PPS was provided to the coders and examined to determine the types of information collected and procedures for collecting information from site visitors, the degree to which it follows FTC guidelines, the manner in which visitor privacy is framed, and the inclusion of justifications for monitoring. Unless otherwise noted, instances when a particular variable was present were coded 1, and instances when a variable was absent were coded 0.

In regard to the information-collection procedures, coders rated whether or not the PPSs stated that visitor information was collected automatically. If so, coders rated whether or not the following types of information were collected: user behavior on the site (e.g., time spent, pages visited), IP address, hardware/software on the visitor’s computer, and other Web sites visited (e.g., the referring site). A total-automatic-collection index was created by summing the total number of the four different types of information automatically collected per PPS ($M = 1.75$; $SD = 1.44$). Coders also rated whether or not visitors were asked to voluntarily submit information about themselves. If so, coders identified the types of information that visitors were asked to provide, including name, contact information, demographic information (e.g., age, gender, etc.), interests (e.g., hobbies), and financial/legal information (e.g., credit card information, social security number). A total-voluntary-collection index was created by summing the total number of the five different types of information voluntarily collected per PPS ($M = 1.68$; $SD = 1.43$). In addition, coders identified the specific instances when visitors were asked to voluntarily provide information, including to become a member or make an information request, and to purchase goods. Finally, coders rated whether or not (according to the PPS) the Web site used cookies and if the term *cookies* was defined (or a link to a definition was provided).

PPSs were also evaluated to determine the degree to which they conform to the five Fair Information Principles established by the FTC. Coders rated whether or not key characteristics that correspond to each of the five principles were addressed in the PPS. PPSs that addressed the notice principle identified when visitors’ information was shared with internal partners (within the organization or business partners) or third parties. The principle of choice was fulfilled if the PPS stated that visitors had a choice (e.g., to opt in or opt out) in how their personal information was used. Access involved allowing visitors to view information collected about themselves. Security included informing participants of the site’s policy regarding information security. Redress involved informing visitors of any mechanisms in place to enforce visitor privacy or steps that visitors should take if they feel that their privacy has been violated. An index was also created by adding

TABLE 1
Web Sites From Which the PPSs in the Sample Were Drawn

<i>Web Site Addresses</i>			
www.aacap.org	www.drgreene.com	www.healthywomen.org	www.muschealth.com
www.aap.org	www.drkoop.com	www.helping.apa.org	www.nal.usda.gov
www.aarp.org/health	www.drugdigest.org	www.hmc.psu.edu/healthinfo	www.nccam.nih.gov
www.about.com/health	www.druginfonet.com	www.holisticwebworks.com	www.nhlbi.nih.gov
www.ahrq.gov	www.drweil.com	www.homepage.mac.com/tgrugle/cyber	www.nia.nih.gov
www.always-health.com	www.ec-online.net		www.niaaa.nih.gov
www.americanheart.org	www.embracingwomenshealth.com	www.hopkinshospital.org	www.nichd.nih.gov
www.anatomyatlases.org	www.eMedicine.com	www.intellihealth.com	www.nida.nih.gov
www.ayurveda-foryou.com	www.estronaut.com	www.kidshealth.org	www.Nimh.nih.gov
www.cancer.gov	www.familydoctor.org	www.labtestsonline.org	www.onpointhealth.com
www.cancer.org	www.girlshealth.gov	www.mayoclinic.com	www.partners.org
www.cancertrack.com	www.healingwell.com	www.mchlibrary.info	www.RxList.com
www.cdc.gov	www.health.discovery.com	www.mcw.edu	www.samhsa.gov
www.cdcnpin.org	www.health.gov/NHIC	www.mdadvice.com	www.sleepfoundation.org
www.cfsan.fda.gov	www.health.ivillage.com	www.mdanderson.org	www.sutterhealth.org/health
www.childrenshospital.org	www.health.msn.com	www.mdlinx.com	www.talkmedical.com
www.chop.edu	www.health.yahoo.com	www.medem.com	www.thebody.com
www.cincinnaticchildrens.org	www.healthatoz.com	www.medhelp.org	www.usa.gov/Citizen/Topics/Health
www.clevelandclinic.org	www.health-care-information.org	www.medicalnewstoday.com	www.walgreens.com/library
www.cnn.com/health	www.healthfinder.gov	www.medicinenet.com	www.web.mel.org
www.columbiastmarys.com	www.healthinfochannel.com	www.medlineplus.gov	www.webmd.com
www.consumerhealthdigest.com	www.healthline.com	www.medscape.com	www.websites.afar.org
www.coolnurse.com	www.healthology.com	www.mentalhelp.net	www.wisegeek.com/health
www.coxhealth.com	www.healthscout.com	www.mentalwellness.com	www.womenshealth.gov
www.cyberdiet.com	www.healthsquare.com	www.merck.com	www.yalemedicalgroup.org
www.cyh.com	www.mdchoice.com	www.mercy.net/healthinfo	www.yourhealthinformation.com
www.diabetes.niddk.nih.gov	www.healthtouch.com	www.moffitt.org	

Note. The total number of Web sites in this list is greater than the number of PPSs in the sample. Twelve of these Web sites were owned by the same companies and have the same PPSs (see footnote 3 for further details). PPS = privacy policy statement.

each of the five characteristics used to assess the FTC's guidelines ($M = 1.67$, $SD = 1.42$). Greater scores on this measure indicate that more of the guidelines were followed by a particular Web site.

Coders rated the manner in which visitor privacy was framed and discussed in the PPS based on two categories identified by Markel (2005). First, the value placed on visitors' privacy was examined. PPSs were coded into three categories: (a) pro-visitor PPSs articulated their concern with visitor privacy (e.g., "We're concerned about, respect, or value your privacy"), (b) pro-organization PPSs recognized that the visitor was concerned with his or her privacy—although the owners were not necessarily concerned (e.g., "You're concerned about or value your privacy"), or (c) neutral PPSs did not editorialize about the value of visitors' privacy. Although Markel does not discuss the third category, it seems plausible that some PPSs may not explicitly editorialize about the value of visitors' privacy. Second, the justifications offered for collecting personal information were examined. Raters coded whether or not the PPS stated why information was being collected. In instances in which a justification

was given, raters coded each reason into one of four possible categories derived from Markel's work, including: to improve the quality of the site, to customize the visitor experience on the site, to enable visitors to buy products or services from the site, and to give or sell visitors' information to others.

To determine intercoder reliability, approximately 30% of the PPSs were independently coded by two trained undergraduate students who served as coders. Scott's pi (Potter & Levine-Donnerstein, 1999), which accounts for intercoder agreement due to chance, was computed to assess intercoder reliability. Scott's pi ranged from .80 to 1.0 for 26 of the 29 variables. Intercoder reliability for the variables assessing one of the instances when personal information was voluntarily requested (to purchase goods), one of the justifications for collecting information (customize the visitor experience on the site), and one of the Fair Information Practice guidelines (access) were .74, .60, and .66, respectively. Disagreements were resolved by discussion. The remaining PPSs were divided equally between the two raters and independently coded.

Finally, PPS readability was assessed with the Flesch-Kincaid (Flesch, 1979) grade-level measure. This formula takes into account the mean sentence length of a document and the mean number of syllables per word.⁵ The output reflects the grade level one must have completed in contemporary U.S. education to understand a particular document ($M = 13.08$, $SD = 1.92$).

RESULTS

Information Included in General-Reference Health Web Sites PPSs

RQ1a and RQ1b asked about the types of information voluntarily and automatically collected. The frequencies relevant to these questions are presented in Table 2. In general, approximately 80% of the health Web sites in the sample reported using voluntary and automatic data collection procedures. At least 40% of the sites automatically collected specific information about visitors' behavior on the site, IP address, hardware or software on the individual's computer, and other Web sites visited. In regard to specific types of information collected voluntarily, approximately 70% of sites collected contact information from visitors.

RQ2 asked about the degree to which general-reference health Web sites conform to the FTC's Fair Information Practice guidelines. The results are displayed in Table 2. Approximately half of the PPSs complied with the notice and security guidelines, explaining when information would be shared and addressing how the information would be secured. Fewer than 30% of sites, however, addressed the choice, access, and redress principles. Of the five different characteristics used to assess the FTC's guidelines, 70% of the PPSs addressed two or fewer, and over 25% of sites addressed none of the guidelines. Only 3% of the PPSs addressed all five of the Fair Information Practice guidelines.

Differences in the Content of PPSs Based on Policy Framing

H1 predicted that Web sites with pro-visitor-framed PPSs would (a) request that visitors voluntarily provide more information and (b) automatically track more information from site visitors than those sites with PPSs that are not explicitly framed as pro-visitor. In addition, RQ3 asked if pro-visitor-framed PPSs were more likely to conform to FTC guidelines. H3a predicted that there would be differences in the readability of PPSs based on the manner in which they were framed. To test these hypotheses and

TABLE 2
Frequency of Information Included in PPSs

<i>PPS Content</i>	<i>Frequency</i>	<i>%</i>
Site type		
.gov, .org, .edu	51	52.6
.com/.net	46	47.4
Information collection: automatic	80	82.5
User behavior on the site	46	47.4
IP address	45	46.4
Hardware/software on a personal computer	40	41.2
Other Web sites visited	39	40.2
Information collection: voluntary	80	82.5
Name	42	43.3
Contact information	70	72.2
Demographic information	26	26.8
Financial/legal information	17	17.5
Interests	8	8.2
When information is requested		
To become a member or make an information request	52	53.6
To purchase goods/services	27	27.8
Cookies addressed	63	64.9
Cookies defined	43	44.3
Justification for collecting information	78	80.4
To improve site quality	59	60.8
To customize the visitor's experience	35	36.1
To enable visitors to buy products or services	4	4.1
To share or sell visitors' information	1	1.0
Fair Information Practices		
Notice	48	49.5
Choice	26	26.8
Access	26	26.8
Security	51	52.6
Redress	11	11.3

Note. $N = 97$. Percentage refers to frequency with which a type of information appears relative to the total number of PPSs analyzed. PPS = privacy policy statement.

answer this research question, those PPSs that were framed as pro-organization ($n = 8$) or neutral ($n = 34$) were combined and compared with PPSs that were explicitly pro-visitor ($n = 52$). Results addressing these hypotheses and this research question are displayed in Table 3.

These data show evidence to support H1a. A one-way analysis of variance (ANOVA) examining the main effect of PPS framing on the total-voluntary-collection index indicated that pro-visitor PPSs ($M = 2.15$, $SD = 1.32$) reported requesting significantly greater amounts of information voluntarily from site visitors than those PPSs that were not framed as pro-visitor ($M = 1.12$, $SD = 1.37$), $F(1, 92) = 13.86$, $p < .01$, $\eta^2 = .13$. In regard to specific types of information, chi-square analyses indicated that pro-visitor PPSs were more likely to report requesting visitors' names,

⁵The formula for the Flesch-Kincaid grade-level readability measure is as follows: $0.39 \times (\text{total words}/\text{total sentences}) + 11.8 \times (\text{total syllables}/\text{total words}) - 15.59$.

TABLE 3
Differences in PPS Content Based on Policy Framing
(Explicitly Pro-Visitor vs. Not Explicitly Pro-Visitor)

Information Type	Pro-Visitor Frequency (%)	Not Pro-Visitor Frequency
Site type*		
.gov, .org, .edu	20 (38.5)	28 (66.7)
.com, .net	32 (61.5)	14 (33.3)
Information collection: automatic		
User behavior on the site*	16 (30.8)	29 (69.0)
IP address	24 (46.2)	20 (47.6)
Hardware/software on a personal computer*	16 (30.8)	24 (57.1)
Other Web sites visited*	12 (23.1)	26 (61.9)
Information collection: voluntary		
Name*	32 (61.5)	9 (21.4)
Contact information*	45 (86.5)	23 (54.8)
Demographic information*	18 (34.6)	7 (16.7)
Financial/legal information*	13 (25.0)	4 (9.5)
Fair Information Practices		
Notice*	32 (64.0)	13 (31.0)
Choice*	18 (34.6)	7 (16.7)
Access	18 (34.6)	8 (19.0)
Security	26 (50.0)	24 (57.1)
Redress	3 (05.8)	7 (16.7)

Note. Percentages were computed for each information type within each group. Accordingly, percentages refer to the frequency with which a particular type of information was included in pro-visitor PPSs (or not explicitly pro-visitor) relative to the total number of PPSs that are pro-visitor (or not explicitly pro-visitor).

* $p \leq .05$.

$\chi^2(df = 1) = 15.20, p < .01$; contact information, $\chi^2(df = 1) = 11.73, p < .01$; demographic information, $\chi^2(df = 1) = 3.83, p = .04$; and financial/legal information, $\chi^2(df = 1) = 3.76, p = .05$. Because fewer than 10 of the PPSs in the sample reported collecting voluntary information regarding visitors' interests, this variable was not analyzed. In addition, it is noteworthy that pro-visitor PPSs were significantly more likely to be from for-profit Web sites (as indicated by a .com domain) than nonprofit sites (as indicated by an .org, .edu, or .gov domain), $\chi^2(df = 1) = 7.40, p < .01$.

H1b, however, was not supported. A one-way ANOVA examining the main effect of PPS framing on the total-automatic-collection index revealed that, contrary to predictions, those PPSs framed as pro-visitor ($M = 1.31, SD = 1.25$) reported collecting significantly less information than PPSs that were not framed as pro-visitor ($M = 2.36, SD = 1.46$), $F(1, 92) = 14.12, p < .01, \eta^2 = .13$. Chi-square analyses indicated that PPSs framed as pro-visitor were less likely to automatically collect information related to visitors' behavior on the site, $\chi^2(df = 1) = 13.64, p < .01$; hardware/software on the visitors' computers, $\chi^2(df = 1) = 6.61, p = .01$; and other Web sites viewed by the visitor, $\chi^2(df = 1) = 14.54, p < .01$. There was no difference in the automatic

collection of visitors' IP addresses, $\chi^2(df = 1) = 0.02, p = .89$, among those PPSs that were and were not explicitly pro-visitor.

To answer RQ3, a one-way ANOVA was conducted that indicated that there was no difference in the total number of FTC guidelines met in those PPSs that were explicitly pro-visitor ($M = 1.87, SD = 1.43$) as compared to those that were not explicitly pro-visitor ($M = 1.40, SD = 1.43$), $F(1, 92) = 2.41, p = .12, \eta^2 = .03$. In regard to specific FTC guidelines, chi-square tests indicated that pro-visitor sites were more likely to explicate their data-sharing practices corresponding to the notice principle, $\chi^2(df = 1) = 9.98, p < .01$, and to offer visitors a choice in how their personal information was used, $\chi^2(df = 1) = 3.83, p = .05$. However, there were no differences between pro-visitor and other types of PPSs in the guidelines pertaining to access, $\chi^2(df = 1) = 2.81, p = .09$; security, $\chi^2(df = 1) = 0.48, p = .49$; or redress, $\chi^2(df = 1) = 2.90, p = .09$.

A one-way ANOVA was conducted to address H3a. The difference between the readability of pro-visitor-framed PPSs ($M = 13.23, SD = 2.00$) and those PPSs that were not framed as pro-visitor ($M = 12.76, SD = 1.73$) was not statistically significant, $F(1, 92) = 1.49, p = .23, \eta^2 = .02$. No support was found for H3a.

Differences in the Content of PPSs Based on the Inclusion of Justifications for Monitoring

H2 predicted that organizations with a PPS including a justification for monitoring visitors would be more likely to (a) request and (b) automatically track more information from visitors than those that did not include a justification. RQ4 asked if those PPSs that included a justification for monitoring were more likely to conform to FTC guidelines. H3b posited that there would be differences in the readability of PPSs based on whether or not a justification was included for collecting data from site visitors. A total of 78 PPSs included at least one justification for monitoring visitors, whereas 19 did not include a justification. Results are displayed in Table 4.

Mixed support was found for H2a. A one-way ANOVA examining the main effect of including a justification for monitoring on the total-voluntary-collection index indicated that PPSs that included a justification ($M = 1.85, SD = 1.44$) reported requesting significantly greater amounts of voluntary information from site visitors than those PPSs that did not include a justification ($M = 1.00, SD = 1.16$), $F(1, 95) = 5.64, p = .02, \eta^2 = .06$. However, there were few differences in the specific types of information requested. The only difference in regard to specific types of voluntary information requested was contact information, $\chi^2(df = 1) = 4.49, p = .03$. There were no differences in requests for visitors' names, $\chi^2(df = 1) = 2.78, p = .10$; demographic information, $\chi^2(df = 1) = 3.19, p = .07$; or financial/legal information, $\chi^2(df = 1) = 2.46, p = .12$; among those sites that did and did

TABLE 4
Differences in PPS Content Based on the Inclusion
of Justification(s) for Monitoring

Information Type	Justification Frequency (%)	No Justification Frequency
Site type		
.gov, .org, .edu	43 (55.1)	8 (42.1%)
.com, .net	35 (44.9)	11 (57.9%)
Information collection: automatic		
User behavior on the site*	43 (55.1)	3 (15.8)
IP address*	41 (52.6)	4 (21.1)
Hardware/software on a personal computer*	38 (48.7)	2 (10.5)
Other websites visited*	37 (47.4)	2 (10.5)
Information collection: voluntary		
Name	37 (47.4)	5 (26.3)
Contact information*	60 (76.9)	10 (52.6)
Demographic information	24 (30.8)	2 (10.5)
Financial/legal information	16 (20.5)	1 (5.3)
Fair Information Practices		
Notice	41 (53.9)	7 (36.8)
Choice	23 (29.5)	3 (15.8)
Access*	25 (32.1)	1 (5.3)
Security*	47 (60.3)	4 (21.1)
Redress	11 (14.1)	0 (0.0)

Note. Percentages were computed for each information type within each group (justification or no justification). Percentages refer to the frequency with which a particular type of information was included in PPSs that included a justification for monitoring (or did not) relative to the total number of PPSs that included a justification for monitoring (or did not).

* $p < .05$.

not offer a justification for monitoring visitors. It is noteworthy that there was no difference in the use of a justification for monitoring between for-profit and not-for-profit Web sites, $\chi^2(df = 1) = 1.04, p = .31$.

H2b was supported. A one-way ANOVA indicated that those PPSs including a justification for monitoring site visitors ($M = 2.04, SD = 1.39$) reported collecting more types of information automatically than those PPSs that did not include a justification ($M = .58, SD = 1.02$), $F(1, 95) = 18.46, p < .01, \eta^2 = .16$. Further, those PPSs that included a justification were more likely to report automatically collecting specific information about visitors' behavior on a site, $\chi^2(df = 1) = 9.48, p < .01$; IP address, $\chi^2(df = 1) = 6.10, p = .01$; hardware/software, $\chi^2(df = 1) = 9.20, p < .01$; and other Web sites visited, $\chi^2(df = 1) = 8.66, p < .01$.

A one-way ANOVA conducted to address RQ4 indicated that those PPSs that included a justification for monitoring ($M = 1.88, SD = 1.43$) also met more of the FTC's guidelines for Web site PPSs than those that did not include a justification for monitoring ($M = .79, SD = .98$), $F(1, 95) = 9.94, p < .01, \eta^2 = .09$. In regard to specific FTC guidelines, chi-square tests indicated that PPSs including a justification for monitoring were more likely to address the access, $\chi^2(df = 1)$

$= 5.59, p = .02$, and security components, $\chi^2(df = 1) = 9.42, p < .01$, of the FTC's guidelines. However, there were no differences between those PPSs that did and did not include a justification in regard to the guidelines pertaining to notice, $\chi^2(df = 1) = 1.78, p = .18$; choice, $\chi^2(df = 1) = 1.46, p = .23$; and redress, $\chi^2(df = 1) = 3.02, p = .08$.

A one-way ANOVA was conducted to test H3b. The results indicated that the difference between the readability of PPSs that included a justification for monitoring ($M = 13.12, SD = 1.95$) and those that did not include a justification ($M = 12.92, SD = 1.84$) was not statistically significant, $F(1, 95) = 0.17, p = .68, \eta^2 < .01$. H3b was not supported.

DISCUSSION

Widespread use of the World Wide Web for health information, care, and services makes understanding the PPSs of health Web sites an important area of research for communication scholars. The results of the study reported here indicate that a variety of information is being routinely collected about visitors by general-reference health Web sites. Moreover, differences in the content of PPSs in the data set based on the manner in which visitor privacy is framed and the inclusion of a justification for monitoring suggests that these two rhetorical strategies may play an important role in constructing the secondary exchange of personal information for Web site access between Web users and health Web sites. These findings and their implications will be discussed in the following paragraphs.

The PPSs from general-reference health Web sites that were analyzed in this study indicate that a majority of sites collected information about site visitors and their behavior. Approximately 80% of PPSs indicated collecting information automatically or requested that visitors voluntarily provide personal information. In regard to specific types of information collected, approximately 40% of the PPSs indicated asking visitors to voluntarily provide their names and almost three-fourths of PPSs noted requesting information about how visitors could be contacted. These two results were fairly similar to what has been reported in previous research on PPSs from direct-to-consumer Web sites for branded pharmaceuticals. Sheehan (2005) found that over half of the sites in her sample requested visitors' names, e-mail addresses, and postal addresses. This study extends previous research on the PPSs of health-related Web sites by also evaluating information about visitors that was automatically collected. Of the PPSs in the sample, 40% or more reported automatically collecting information about visitors' behavior on the site, IP address, hardware or software on their computer, and other Web sites they visited.

Although, at first glance, much of the data collected by the Web sites in the sample appears to be fairly innocuous, the widespread collection of information about visitors to health Web sites has important implications for Web users

and health practitioners. Information regarding visitors' finances or the types of pages visited on a particular Web site could be worrisome to information seekers—especially given the potential for information pooling or sharing (Choy et al., 2001). One specific concern is the possibility of a privacy breach or the release of potentially sensitive information (Anton & Earp, 2001). Revealing the details of an individual's search for information about a particular health topic such as a sexually transmitted infection or mental illness could have consequences ranging from embarrassment to affecting one's employment.

Beyond the sheer amount of information collected, the results of this study offer insights into the way that privacy is constructed in Web site PPSs. In particular, the results provide some evidence consistent with the notion that PPSs are a persuasive tool used by organizations to help facilitate the secondary exchange of personal information for Web site access (LaRose & Rifon, 2006; Markel, 2005). There was a relationship between the way in which visitors' privacy was framed and the inclusion of justifications in PPSs and the Web site's data-collection practices. Sites that included a justification in their PPS for collecting information were more likely to collect information automatically and voluntarily from visitors. In addition, personal information was more likely to be voluntarily requested from visitors by organizations with a PPS that was framed as pro-visitor. These results are partially consistent with LaRose and Rifon's (2006) finding that the number of justifications offered in PPSs for monitoring was positively correlated with the number of different involuntary privacy disturbances to which consumers were exposed (e.g., tracking a visitor's IP address, leaving cookies). Taken as a whole, the results from this study are consistent with the notion that offering justifications for monitoring, and to a lesser extent the way a PPS is framed, are rhetorical tropes used by health organizations to encourage site visitors to engage in the information-for-access transaction. The findings also reinforce the notion that the secondary exchange is likely subjective. As such, offering a justification could minimize the perceived risks associated with revealing personal information and make it possible to gather large amounts of personal information from and about consumers.

The results also suggest that the framing of PPSs may be more than face-work on the part of the organization or individual operating the health Web site. Contrary to predictions, several types of information were less likely to be automatically collected by sites with a PPS framed as pro-visitor. Further, those sites that were framed as pro-visitor or that included justifications for monitoring were more likely to follow the Fair Information Practice guidelines. This result is informative in that it underscores the complex tension faced by organizations operating a health Web site between protecting visitors' interests and the necessity of information collection. Creating an attractive and effective health Web site can be greatly facilitated if organizations

know who is visiting their site and how these individuals are using it; yet collecting detailed information about Web-site visitors and their behavior risks encroaching on visitors' privacy and undermining perceptions of the Web site. The use of PPS framing among the Web sites in this sample may reflect an attempt at managing this tension.

The results of the analyses indicate that the PPSs in the sample do not closely follow the FTC's Fair Information Practice guidelines. Only 3% of the PPSs addressed all five guidelines. Further, less than 30% of PPSs addressed choice, access, or redress. Half or more of the PPSs in the sample, however, did address the notice and security guidelines. This general pattern of findings is fairly consistent with the results of Sheehan's (2005) study of direct-to-consumer pharmaceutical Web sites. In addition, the results in regard to notice and security are consistent with the FTC's analysis of 335 PPSs from randomly selected consumer goods and services Web sites in 2000; however, the choice and access guidelines were met in a smaller portion of the PPSs in this sample than in the FTC study. Taken as a whole, the results suggest that, although a fair amount of time has passed since they were created, Web sites have not gotten better about meeting the FTC's Fair Information Practices guidelines and articulating their privacy practices to visitors.

Although there were no differences in the readability of the PPSs in the sample based on how visitor privacy was framed or the inclusion of justifications for monitoring, it is noteworthy that the mean level of readability was quite high. The PPSs in this sample were written at a level that requires at least a high school education to understand. Unfortunately, this result is similar to Milne et al.'s (2006) longitudinal study of PPS readability during 2001 and 2003 and reflects a disconcerting trend. The high level of education required to understand health Web site PPSs undermines the FTC's Fair Information Principles by obfuscating the very data-collection and use practices that the Principles were constructed to elucidate.

The results of this study suggest some straightforward implications and recommendations for practitioners of health communication and information seekers. First, consumers should be made aware of the extensive data-collection practices of health Web sites. Although 80% of the PPSs in the sample indicated that information about consumers was collected automatically, Turow's (2003) research indicates that many Internet users are not aware of these practices. As such, many consumers may be unknowingly providing information regarding their Web-use behavior. In formulating guidelines for effective information seeking online, such as those produced by the National Center for Complementary and Alternative Medicine (2006) and MedlinePlus (2004), it is important to make it explicit to potential information seekers that they are being monitored even if they do not register at a Web site or voluntarily provide information.

A second recommendation suggested by the results of this study is that consumers should be made aware of the tropes used in PPSs to shape their perceptions of privacy and the commensurate implications for the site's data-collection practices. In particular, PPSs stating that the organization has site visitors' interests at heart may very well act in their best interests. The results of this study suggest that sites framed in this way may be less likely to automatically collect information and more likely to meet the FTC's Fair Information Practice guidelines. However, those sites that include justifications for data collection were more likely to encroach on visitors' privacy. Organizations including justifications in their Web site PPSs may be more likely to collect information automatically and voluntarily from visitors.

The preceding discussion must be considered in light of the limitations of this study. In particular, the Web site PPSs analyzed in this study were not randomly sampled. Although we reviewed over 600 health Web sites, we could not determine the population of general-reference health Web sites and therefore could not produce a random sample of such sites. Nonetheless, we feel that the sample is of merit. The data set was selected in a manner that reflects the typical American's information-seeking behavior and included some of the most widely used health Web sites in the world. Further, because we focused on general-reference sites that address a variety of different health issues, we feel that the sample included those health Web sites that are more likely to be used by health consumers. A second potential limitation is that the data for this study consisted of the privacy practices documented in Web site PPSs. There may be some inconsistencies between what companies report in their PPSs and their actual practices in regard to visitor privacy. Given the goals of this study, however, we felt it important to focus on the content of PPSs. A final limitation of the study is that the large number of tests we conducted increased the family-wise error rate and therefore the likelihood of a Type I error.

The results of this study also suggest a few directions for future research. First, it would be worthwhile to assess Web users' evaluations of the importance of different privacy characteristics. That is, is the typical Web user more or less averse to sharing some types of information than others? It may be that users are willing to voluntarily submit contact information such as their e-mail addresses but feel wary of a Web site tracking their use of a Web site. Second, given the differences in PPS content based on the way visitors' privacy was framed and the inclusion of justifications, it would be worthwhile to explore how policy framing and the use of justifications influences users' behavior. For example, are individuals more willing to voluntarily submit information to a site when the PPS is explicitly pro-visitor? Finally, future research should examine PPSs and Web-based privacy practices from the institution's perspective. It would be worthwhile to better understand the perceptions, intentions, and goals of those constructing health Web site PPSs.

Increased use of the Internet and World Wide Web for medical purposes has raised a number of challenges and opportunities for scholars of health communication. One such challenge is to better understand the information and privacy concerns of those venturing online for health purposes. This study represents one step in this endeavor by exploring the PPSs of general-reference health Web sites. Future research is necessary to understand this important topic and, thus, health communication in the information age.

REFERENCES

- Anton, A., & Earp, J. (2001). *A taxonomy for website privacy requirements* (Tech. Rep. No. TR-2001-14). North Carolina State University. Retrieved November 1, 2006, from <http://www.csc.ncsu.edu/faculty/anton/publications.html>
- Bagozzi, R. P. (1975). Marketing as exchange. *Journal of Marketing*, 39, 32-39.
- Baumer, D., Earp, J. B., & Payton, F. C. (2000). Privacy of medical records: IT implications of HIPAA. *ACM Computers and Society*, 30, 40-47.
- Choy, A., Hudson, Z., Pritts, J., & Goldman, J. (2001). Exposed online: Why the new federal health policy regulation doesn't offer much protection to Internet users. *Pew Internet & American Life Project*. Retrieved December 1, 2006, from http://www.pewinternet.org/PPF/r/49/report_display.asp
- Cline, R. J., & Haynes, K. M., (2001). Consumer health information seeking on the Internet: The state of the art. *Health Education Research*, 16, 671-692.
- Consumer Online Privacy and Disclosure Act of 2001. H.R. 347, 107th Cong. (2001).
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59, 323-342.
- Department of Health and Human Services. (2000, December). *Standard for privacy of individually identifiable health information; Final rule*. Retrieved December 1, 2006, from <http://www.hhs.gov/ocr/hipaa/finalreg.html>
- Fallows, D. (2005). How women and men use the Internet. *Pew Internet & American Life Project*. Retrieved June 15, 2007, from http://www.pewinternet.org/pdfs/PIP_Women_and_Men_online.pdf
- Flesch, R. (1979). *How to write in plain English: A book for lawyers and consumers*. New York: Harper & Row.
- Fox, S. (2006). Online health search 2006. *Pew Internet & American Life Project*. Retrieved December 1, 2006, from http://www.pewinternet.org/PPF/r/190/report_display.asp
- Fox, S., & Rainie, L. (2000). The online health care revolution. *Pew Internet & American Life Project*. Retrieved June 15, 2004, from http://www.pewinternet.org/PPF/r/26/report_display.asp
- Gandy, O. (1996). Coming to terms with the panoptic sort. In D. Lyon & E. Zureik (Eds.), *Computers, surveillance, and privacy* (pp. 132-155). Minneapolis: University of Minnesota Press.
- Goldman, J., & Hudson, Z. (2000). Virtually exposed: Privacy and e-health. *Health Affairs*, 19, 140-148.
- Gurak, L. J., & Hudson, B. L. (2006). E-health: Beyond Internet searches. In M. Murero & R. E. Rice (Eds.), *The Internet and health care: Theory, research and practice* (pp. 29-48). Mahwah, NJ: Lawrence Erlbaum Associates, Inc.
- Hong, T., McLaughlin, M., Pryor, L., Beaudoin, C. E., & Grabowicz, P., (2005). Internet privacy practices of news media and implications for online journalism. *Journalism Studies*, 6, 15-28.
- Houston, F. S., & Gassenheimer, J. B. (1987). Marketing and exchange. *Journal of Marketing*, 51, 3-18.

- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*, 263–291.
- LaRose, R., & Rifon, N. (2006). Your privacy is assured—of being disturbed: Websites with and without privacy seals. *New Media and Society*, *8*, 1009–1029.
- LaRose, R., & Rifon, N. (2007). Promoting *i*-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs*, *41*, 127–149.
- Markel, M. (2005). The rhetoric of misdirection in corporate privacy-policy statements. *Technical Communication Quarterly*, *12*, 197–214.
- MedlinePlus. (2004). *MedlinePlus guide to healthy Web surfing*. Retrieved June 16, 2004, from <http://www.nlm.nih.gov/medlineplus/healthyweb-surfing.html>
- Metzger, M. J. (2004). Exploring the barriers to electronic commerce: Privacy, trust, and disclosure online. *Journal of Computer-Mediated Communication*, *9*(4). Available at <http://jcmc.indiana.edu/vol19/issue4/metzger.html>
- Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research*, *33*, 155–179.
- Metzger, M. J., & Docter, S. (2003). Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting and Electronic Media*, *47*, 350–374.
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*, 15–29.
- Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy and Marketing*, *25*, 238–249.
- Mundy, D. P. (2006). Customer privacy on UK healthcare websites. *Medical Informatics and the Internet in Medicine*, *31*, 175–193.
- National Center for Complementary and Alternative Medicine. (2006). 10 things to know about evaluating medical resources on the Web. Retrieved June 20, 2006, from <http://nccam.nih.gov/health/webresources/>
- National Telecommunications and Information Administration. (2000). *Falling through the Net: Toward digital inclusion*. Retrieved July 1, 2006, from <http://www.ntia.doc.gov/ntiahome/fttn00/contents00.html>
- O'Harrow, R. (2001, July 4). Prozac maker reveals patient e-mail addresses. *The Washington Post*, p. E01.
- Potter, W. J., & Levine-Donnerstein, D. (1999). Rethinking reliability and validity in content analysis. *Journal of Applied Communication Research*, *27*, 258–284.
- Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of Web privacy seals on trust and false assurances. *Journal of Consumer Affairs*, *39*, 337–360.
- Ryker, R., Lafleur, E., Cox, C., & McManis, B. (2002). Online privacy policies: An assessment of the Fortune e-500. *Journal of Computer Information Systems*, *42*, 15–20.
- Sheehan, K. (2005). In poor health: An assessment of privacy policies at direct-to-consumer websites. *Journal of Public Policy & Marketing*, *24*, 273–283.
- Thibault, J., & Kelley, H. H. (1959). *The social psychology of groups*. New York: Wiley.
- Turner, B. (2003). Social capital, inequality and health: The Durkheimian revival. *Social Theory and Health*, *1*, 4–20.
- Turow, J. (2003). Americans and online privacy: The system is broken. *Annenberg Public Policy Center*. Retrieved June 8, 2007, from <http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf>
- Turow, J., & Hoofnagle, C. J. (2006, November). The FTC and consumer privacy in the coming decade. Paper presented at the Federal Trade Commission Meeting, "Protecting Consumers in the Next Tech-ade."
- Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*, 431–453.
- Wood, F. B., Benson, D., LaCroix, E., Siegel, E. R., & Fariss, S. (2005). Use of Internet audience measurement data to gauge market share for online health information services. *Journal of Medical Internet Research*, *7*(3), Article e31. Retrieved December 1, 2006, from <http://www.jmir.org/2005/3/e31/>