Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online

Article *in* SSRN Electronic Journal · January 2014

DOI: 10.2139/ssrn.2518581

CITATIONS
2

READS
93

1 author:

Kirsten E. Martin
University of Notre Dame
61 PUBLICATIONS **1,298** CITATIONS

SEE PROFILE

Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online

Kirsten Martin

Recent privacy scholarship has focused on the failure of adequate notice and consumer choice as a tool to address consumers' privacy expectations online. However, there has not been a direct examination into how complying with a privacy notice is related to meeting privacy expectations online. This article reports the findings of two factorial vignette studies describing online consumer tracking, whereby respondents rated the degree to which online scenarios met their privacy expectations or complied with a privacy notice. The results suggest that respondents perceived the privacy notice as offering greater protections than it actually did. Perhaps most problematically, respondents projected the important factors of their privacy expectations onto the privacy notice. In other words, privacy notices became a tabula rasa for users' privacy expectations. The findings provide guidance for policy makers and firms to avoid unnecessary privacy violations caused by an overreliance on privacy notices. Considering the importance of privacy notices in managing privacy online, more work should extend this study to shed light on how consumers understand notices and how their perceptions of privacy notices map to their privacy expectations, if at all.

Keywords: privacy, notice, privacy statements, business ethics, Fair Information Practice Principles

Online Supplement: http://dx.doi.org/10.1509/jppm.14.139

Firms increasingly track consumers online in retail and marketing efforts. The digitalf marketing industry is worth $62 billion (Dwoskin 2013), and Internet advertising, which reached $43 billion in 2013, is central to marketing strategies (Beales and Eisenach 2014). To make online marketing seamless and efficient, marketers "surreptitiously and inextricably" couple consumer tracking and marketing (Milne, Bahl, and Rohm 2008; see also Beales and Eisenach 2014).[1] The scope of the digital marketing industry and online advertising in particular led Digital Marketing Association chief executive officer Linda Woolley to note, "If public policy decision makers muck around in this area, we really really believe they will do it at their own peril—and at the peril of the growth of the US economy" (Dwoskin 2013; see also DMA Data-Driven Marketing Institute 2013).

Yet online privacy and consumer tracking has been the subject of recent public policy scrutiny across a broad array of government agencies (FTC 2012, 2014; U.S. Government Accountability Office 2013; White House 2012, 2014). Online privacy persists as a public policy issue because consumers remain concerned about online behavioral advertising and related tracking (Leon et al. 2013; McDonald and Cranor 2008; Ur et al. 2012). In other words, many Internet users dislike being tracked (Agarwal et al. 2013; Rainie et al. 2013), and people care about the scope and sharing of even innocuous information (Leon et al. 2014). Online tracking rightly remains the focus of consumer advocates and public policy makers (Miyazaki 2008).

Fair Information Practice Principles (FIPPs) have been the primary tools within public policy and practice to address privacy expectations online. Although the "notice-and-choice model" within FIPPs has an alternative—the

[1]To fulfill marketers' needs for individualized information, data brokers collected 1.4 billion consumer transactions and 700 billion aggregated data elements in 2013 (Federal Trade Commission [FTC] 2014).

Kirsten Martin is Assistant Professor, Strategic Management and Public Policy, George Washington University (e-mail: martink@gwu.edu). This material is based on work supported by the National Science Foundation under Grant No. 1311823. Helen Nissenbaum and the NYU Privacy Research Group were invaluable in providing feedback on an earlier version of this article and in broadening the implications. In addition, the manuscript was improved through feedback from Mary Culnan, Howard Beales, Pedro Leon, and the attendees at the 2013 Privacy Law Scholars Conference as well as the 2013 Academy of Management annual meeting. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation. Josh Weiner served as associate editor for this article.

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

Journal of Public Policy & Marketing, Ahead of Print
DOI: 10.1509/jppm.14.139

harm-based model (Beales and Muris 2008; Muris 2001), which focuses on specific harms to the consumer—the FTC's recent guidance retains a focus on notice and choice (Ohlhausen 2014b). Notice and choice are viewed as core to FIPPs in policy (FTC 2010, 2012) and in practice (Culnan and Armstrong 1999; Culnan and Williams 2009; Peslak 2005; Sheehan 2005). In summary, privacy notices and consumer choice are the current key principles for respecting and protecting privacy online (Cranor 2012).

The notice-and-choice model's utility has strained with the added pressure of consumer tracking techniques and online advertising. As summarized by FTC Commissioner Maureen K. Ohlhausen (2014b, p. 7; see also Ohlhausen 2014a), the "challenge [for policy] … is developing the right market solutions or new regulatory approaches that will permit beneficial uses of data while meeting the wide range of consumer preferences for privacy" Moreover, the reliance on notice-and-choice needs to reflect changes in technology and the marketplace (U.S. Government Accountability Office 2013).

Indeed, there is considerable agreement that the notice-and-choice model has failed to meet the privacy expectations of users online (Nissenbaum 2011), yet little has been done to map out specifically how compliance with a privacy notice meets privacy expectations, if at all. The goal of this article is to determine whether and how judgments about privacy expectations online are related to judgments about compliance with privacy notices with respect to online tracking. The disconnect between meeting users' privacy expectations and complying with a given privacy notice can be striking: of surveyed websites, 61% transmitted identifying information to at least one outside web domain, and 45% of websites transmitted information to at least four additional organizations online, in compliance with their policies (Angwin 2011; Mayer 2014); however, a majority of users (68%) have stated that they never approve of being tracked online (Turow et al. 2009). To move forward, public policy makers and firms need to understand how privacy notices compare with users' privacy expectations.

To examine whether and how judgments about privacy expectations differ from judgments about privacy notice compliance, two factorial vignette studies were conducted covering online consumer tracking. Respondents rated the degree to which online scenarios met consumers' privacy expectations (N = 485 respondents and 19,400 vignettes) or complied with a privacy notice (N = 488 respondents and 19,520 rated vignettes). The findings suggest that consumers perceive their privacy expectations to be included in the privacy policy even when the actual notice differs considerably.

This study directly supports public policy and the FTC's mission to protect consumer privacy. The empirical examination of consumer privacy expectations and perceptions of privacy notices addresses two recently identified research needs within public policy regarding privacy online (Ohlhausen 2014b, p. 8). First, research should "shed light on consumer attitudes and preferences regarding privacy choices" to better inform public policy. Second, research should provide "empirical evidence on how consumers perceive and understand privacy-related disclosures" to help regulators understand the role of privacy notices for consumers. This study directly compares consumer preferences and expectations with how consumers perceive and understand privacy statements.

The results have implications for firms online as well as for privacy scholars in marketing management, public policy, and business ethics. The results show that a reliance on privacy notices to meet consumers' privacy expectations seems to provide a necessary, but not sufficient, condition for meeting privacy expectations. When people find privacy notices to be insufficient in meeting their privacy expectations, they have attempted to pull out of this information exchange and obfuscate their behavior using tools such as CacheCloak, donottrack.us (Mayer and Narayanan 2012), BitTorrent Hydra, TOR, and TrackMeNot (Brunton and Nissenbaum 2011), which enable users to maintain their privacy expectations regardless of a website's privacy policy. Understanding how, if at all, judgments about privacy notices are related to privacy expectations should help firms avoid unnecessary and unintentional privacy violations caused by an overreliance on privacy notices.

Privacy Expectations and Privacy Notices

Privacy Expectations

Marketers and firms navigate an increasingly complicated maze of laws and regulations in regard to privacy. Firms must take into consideration laws such as the Children's Online Privacy Protection Rule (COPPA), the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA) in addition to the ubiquitous FIPPs primarily regulated by the FTC, as mentioned previously. Firms are assessed for their compliance with laws and regulations—for example, their compliance with notice requirements of FIPPs (Sheehan 2005; Culnan 2000) and the readability of their notice (Milne, Culnan, and Greene 2006). Such legalistic approaches to privacy examine the degree to which the firm is compliant with the law or regulation (Goodwin 1991).

A growing area of scholarship focuses on consumer privacy expectations of information practices in marketing and public policy. Rather than assess whether firms meet legal requirements, firms are judged on whether they meet consumers' privacy expectations. For example, Milne and Rohm (2000) shift from investigating whether firms comply with FIPPs to examine how consumers *perceive* firms' compliance with FIPPs. The examination of consumers' privacy expectations in general (Milne and Bahl 2010; Phelps, Nowak, and Ferrell 2000) and privacy expectations about specific technologies such as cookies (Miyazaki 2008) shift from focusing on how well a firm complies with rules and regulations to how consumers perceive firms' information practices. Complicating the examination of privacy expectations is that such expectations can vary by context, platform, and, importantly, individual disposition. For example, Hoffman, Novak, and Peralta (1999) analyze consumer privacy expectations as dependent on the medium of the information exchange (see also Martin 2012a).

Consumer privacy expectations, or consumers' preferences and desires about information privacy, have become increasingly important in a self-regulating environment. For privacy expectations scholarship, the important metric for firms is then defined by the consumer rather than by regulators. Moreover, in a self-regulating environment, it is important for firms to manage whether they meet consumer privacy expectations (Petty 2003), whereby the "congruency of [privacy] expectations can lead to higher levels of trust and a more munificent environment for all" (Milne and Bahl 2010, p. 138).

In addition, the close examination of consumer privacy expectations is important for firms to possibly influence privacy expectations through compensation (Gabisch and Milne 2014) and to find a balance between invasive marketing tactics and consumers' privacy expectations (Petty 2003). Extending this scholarship about consumer privacy expectations requires "testing the relationship between various firm-level practices and their affects on consumers' privacy perceptions" (Lanier and Saini 2008), as is the focus here.

Although privacy is difficult to define (Goodwin 1991; Solove 2006), privacy expectations have been recently defined as the social norms within particular information contexts (Nissenbaum 2009). Privacy as contextual integrity suggests that privacy expectations are the contextual rules about information within specific communities (Nissenbaum 2009). Those privacy norms dictate which data are acceptable to collect, who can have access, whether the information should be kept confidential, and how it can be shared and reused. Such privacy expectations are formed within a social contract (Culnan 1995; Dunfee, Smith, and Ross 1999; Martin 2012; Milne and Gordon 1993; Miyazaki 2008), in which communities develop rules about disclosure and dissemination of information (Phelps, Nowak, and Ferrell 2000). Within any context or community, meeting privacy expectations is important for consumers to be treated fairly, to avoid harm, and to maintain trust.

Privacy Notices

The notice-and-choice model, also known as "awareness" and "control" (Milne 2000), relies on privacy statements and policies for effective consumer notice of firm practices (Cranor 2012; Cranor et al. 2014; Milne and Culnan 2004). Privacy statements have proven effective in engendering consumer trust (Tang, Hu, and Smith 2008), increasing purchase intentions (Miyazaki and Fernandez 2000), and affecting the willingness both to disclose information (Phelps, Nowak, and Ferrell 2000) and to pay for products and services (Tsai et al. 2011).

Yet the effectiveness of privacy statements continues to come under fire, and previous work has explored why notices fail to address privacy expectations specifically. Privacy notices are long, difficult to read, and likely to be ignored (Calo 2012; Martin 2013; Milne and Culnan 2004; Nissenbaum 2011). In addition, they may be unavailable to users (Ur et al. 2012) and unrealistically time intensive (McDonald and Cranor 2008). Research has found privacy statements to be more difficult to understand than the average issue of the *New York Times* and to require two years of college education to comprehend (Sheehan 2005). Indeed, in an empirical study of privacy notices, even law students who were paid to read notices could not understand the terms of the privacy notices (Marotta-Wurgler 2014). Furthermore, these issues are not improving: privacy statements have been found to decline in readability over time (Milne, Culnan, and Greene 2006). Whereas previous scholarship has addressed *why* notices fail to address privacy expectations, the current article is an attempt to understand *how* notices fail to address consumer privacy expectations.

This study addresses the following research question: How are judgments about privacy expectations online related to judgments about complying with privacy notices? For a given situation online, scholars can capture the degrees to which the scenario (1) meets users' privacy expectations and (2) is judged to comply with the privacy notice. As such, judgments about privacy expectations online can be compared with judgments about compliance with privacy notices along two dimensions: the judgments themselves as well as the factors that influence consumers' privacy expectations and their relative importance to consumers' judgments (Jasso 2006).

Relationship Between Privacy Expectations and Privacy Notices

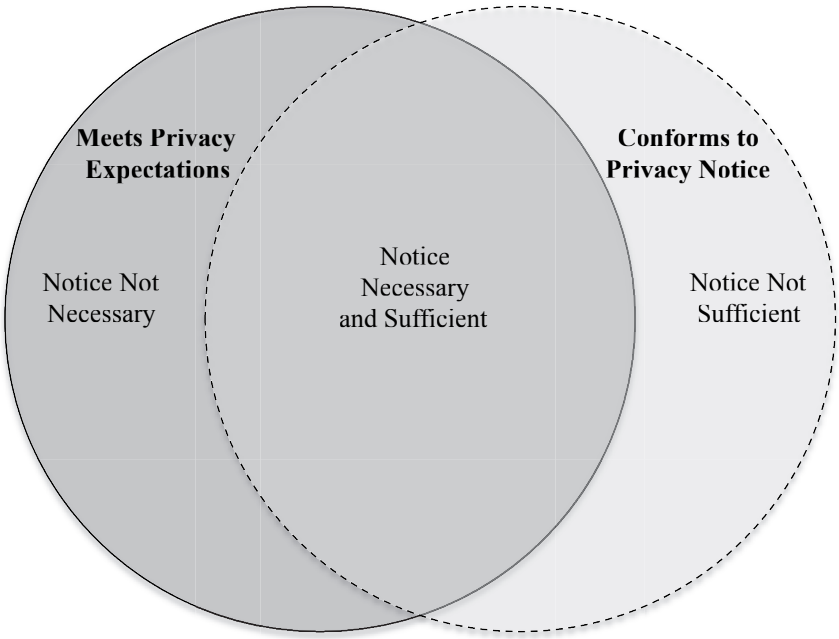
Overall Judgments

Although popular, privacy notices may be immaterial to assessments about the (in)appropriateness of the information transmitted within a particular context. In other words, employees, users, and consumers make judgments about privacy expectations and violations regardless of the privacy notice in many situations.

Indications from regulators, academics, and consumers suggest that notice and choice are neither necessary nor sufficient to meet online privacy expectations. First, as Beales and Muris (2008) report, notice and choice may be unnecessary for many of the most common transactions, such as when completing an automated teller machine transaction (notice is not necessary), filing taxes (choice is not necessary), or credit reporting (neither notice nor choice is necessary). People regularly give information without notice or choice and without believing that their privacy is being violated. In addition, notice and choice are often not sufficient. Privacy policies are often not read, as anecdotally noted by Chief Justice John Roberts when he stated that he does not read end-user agreements (Weiss 2010). Current academic research supports this notion: fewer than 2 of 1,000 shoppers access any privacy agreement, and those that do spend little time reading it (Bakos, Marotta-Wurgler, and Trossen 2014). Yet the effectiveness of notice and choice depends on the assumption that people will read and understand the policies.

Figure 1 depicts the theoretical relationship between privacy notices and privacy expectations. Regulators and firms focused on the notice-and-choice model assume that the circles of Figure 1 overlap, whereby complying with privacy notices is akin to meeting users' privacy expectations. Particularly problematic for consumers is the lighter shaded area in Figure 1, whereby the notice is judged not sufficient to meet privacy expectations; in such cases, practices con-

Figure 1. Relationship Between Meeting Privacy Expectations and Conforming to Privacy Notice



form to a privacy notice yet do not meet consumers' privacy expectations.

Although Figure 1 depicts an equal chance of the privacy notice being insufficient or not necessary in meeting privacy expectations, in actuality firms regularly fail to meet users' privacy expectations while conforming to privacy notices. Indeed, privacy notices are purposefully designed to remain vague to allow for future tracking and targeting techniques and to accommodate future technological capabilities. The details about who the actors are and how the information is transmitted online are obscure, with many indirect third-party organizations involved. In addition, policies change to incorporate technological upgrades or novel privacy measures and become byzantine as a result (Hull, Lipford, and Latulipe 2011). It would therefore be expected that scenarios of online user tracking would be judged as conforming to a privacy notice to a greater degree than judged as meeting privacy expectations.

H_1: Scenarios of online tracking are judged to comply with the privacy notice to a greater degree than they are judged to meet users' privacy expectations.

Factors That Influence Judgments

Two types of factors influence judgments about privacy norms and expectations. First, individual dispositions about privacy, as popularly conceptualized by Westin's (1991) surveys of privacy preferences among the U.S. population, place people on a spectrum between privacy fundamentalists and the privacy unconcerned. Privacy's conceptualization as an individual-level attribute continues in surveys and studies that ask consumers general questions about privacy preferences (Boyles, Smith, and Madden 2012; Urban, Hoofnagle, and Li 2012), privacy concerns (Smith, Milberg, and Burke 1996), and valuation of privacy (Acquisti, John, and Loewenstein 2013; Acquisti and Varian 2005; Chellappa and Sin 2005). According to this research, people vary with regard to their overall belief that privacy is important, and this belief influences their judgments about particular situations.

Here, similar results would be expected for judgments about privacy expectations but not necessarily for judgments about conforming to privacy notices. The measure of how well a scenario meets privacy expectations requires the user to compare the scenario with an internally maintained set of criteria—a set of standards that may vary across individuals (Smith, Milberg, and Burke 1996). However, judgments about conforming to privacy notices should not be as affected by such individual factors. When judgments about privacy expectations are based, in part, on an individually developed disposition, judgments about conforming to a privacy notice utilize an external criterion: the privacy notice itself. Indeed, notices are designed to ensure that the firm's privacy policies are commonly understood by all (Cranor 2012; Milne and Culnan 2004). Therefore, the role of individual-level factors would be greater for privacy expectations relative to judgments about compliance with a privacy notice.

H_2: Individual factors, such as a person's institutional trust and general belief that privacy is important, affect the meeting of users' privacy expectations more than judgments about compliance to a privacy notice.

In addition to privacy as an individual-level disposition, privacy expectations may be contextually defined. For example, privacy expectations may vary by location, such as public versus private space (Nissenbaum 2004); by the type of technology (Hoffman, Novak, and Peralta 1999); or by the novelty of technology (Martin 2012b). Location-based privacy expectations would suggest that all activity online carries similar privacy expectations. A more extreme version of these expectations would suggest that the very act of being online indicates a willingness to relinquish privacy expectations (Acquisti, John, and Loewenstein 2013).

Recent work has examined privacy as contextual integrity, suggesting that it is measured as contextual rules about information (Nissenbaum 2009). A context-specific definition of privacy, or a social contract approach to privacy expectations (Culnan and Bies 2003; Li, Sarathy, and Xu 2010; Martin 2015; Xu et al. 2009), suggests that rules for information flow take into account the purpose of the information exchange as well as the risks and harms associated with sharing information. Rather than measuring privacy concerns and expectations as an attribute of users or the location of the exchange, contextual factors such as the type and use of information would affect privacy judgments.

Privacy notices, however, are viewed as being less specific than contextual privacy expectations. In the analysis of privacy notices, research has found silence on a particular issue, ambiguous language, or broad "change-of-terms" clauses permitting notices to allow almost every type information flow (Bakos, Marotta-Wurgler, and Trossen 2014; Cranor et al. 2014; Marotta-Wurgler 2014; McDonald et al. 2009). Even if people do read notices, organizations are limited in effectively communicating to consumers how information flows online, and consumers often do not understand the notice statements (Leon et al. 2012). Organizations with the best of intentions to notify users struggle to communicate complicated and changing policies that, given the large network of actors in the online space, may conflict with the policies of their online partners such as ad networks, third-party organizations, and user-generated applications (Barocas and Nissenbaum 2009).

Indeed, the more specific the privacy policy (e.g., a policy that includes the type of information and how it is used), the less agreement consumers have in interpreting the notice, and the greater chance that the notice will be misunderstood by the average consumer (Reidenberg et al. 2014); that is, respondents miss the nuances of the policy (Kelley et al. 2010). When privacy expectations are highly dependent on contextual factors, such as the type of information and how it is used, consumers' judgments about privacy notices are typically broad and do not take the particular context into consideration.

H_3: Contextual factors, such as what information is collected, how it is used, and who has access to it, affect judgments about the meeting of users' privacy expectations more than judgments about compliance with a general privacy notice.

Methods

Because the goal of this research is to examine whether and how judgments about privacy expectations differ from judgments about the privacy notice, the study utilizes the factorial vignette survey methodology developed to investigate human judgments (Jasso 2006; Rossi and Nock 1982; Wallander 2009). Though it is established within the field of sociology (Jasso 2006; Rossi and Nock 1982; Wallander 2009), the factorial vignette survey technique is less known within marketing or public policy. The methodology has been used in sociology to shed light on such issues as political action (Jasso and Opp 1997), conceptions of mental illness (Thurman, Lam, and Rossi 1988), factors important to judges' decisions (Hagan, Ferrales, and Jasso 2008), and fairness of compensation (Jasso 2006). In business ethics, the method has been used to examine factors important to stakeholder trust (Pirson, Martin, and Parmar 2014). Factorial vignette methodology assumes "some level of agreement among people in a small group/community as to a combination of factors that is important to take into consideration when making a judgment" (Wallander 2009, p. 514), which renders the methodology particularly well suited to the examination of the relative importance of contextual factors in forming privacy judgments.

In a factorial vignette survey, a set of vignettes is generated for each respondent. The vignette factors, or independent variables, are controlled by the researcher and randomly selected. Respondents are asked to evaluate a series of hypothetical situations with a single rating task—in this case, the degree to which the described scenario either meets the respondent's privacy expectations or conforms to a privacy notice. The methodology supports the researcher in examining (1) the factors used to form judgments, (2) the weight of each of these factors, and (3) how the different groups of respondents agree on the first two items (Nock and Guterbock 2010). These factors and their associated coefficients are referred to as respondents' "equations inside the head" (Jasso 2006). By examining the respondents' equations inside the head, the study aims to learn how they form judgments about privacy expectations and compliance with privacy notices across different online situations.

The factorial vignette survey methodology is uniquely suited to examine consumers' expectations about privacy. First, this study assumes that privacy is highly contextual and that people require a situation's particulars to make a privacy assessment. The factorial survey methodology allows for the simultaneous experimental manipulation of a large number of factors through the use of a contextualized vignette (Ganong and Coleman 2006), which renders the method well suited to the examination of highly contextual concepts such as privacy, in which norms should vary in line with particular online situations. Second, the survey covers an area—privacy—that is fraught with respondent bias, whereby respondents inflate their concern for privacy, which may not reflect their true attitude (Hui, Teo, and Lee 2007). The factorial vignette survey methodology is designed to avoid respondent bias by *indirectly* measuring the respondents' privacy factors and their relative importance. The respondents are not explicitly asked whether selling information is appropriate; rather, respondents read a vignette in which selling information is included among other factors and are asked to rate that scenario. By asking respondents to rate multiple (40) vignettes, the respondents'

privacy factors and their relative importance are identified without directly asking for a ranking. Third, people often have difficulty articulating the factors that constitute their privacy expectations and their relative importance. As an FTC (2010, footnote 72) report notes, traditional surveys are limited in their ability to measure people's privacy expectations.

The vignettes for this study were constructed by varying several online privacy factors for tracking users online. A deck of 40 vignettes for each respondent was randomly created with replacement as the respondent took the survey. For each rated vignette, the associated rating, factor levels, vignette script, and vignette sequence number were preserved. The vignette formats are provided in Appendices A and B with a sample vignette and the vignette template. Each respondent was assigned one type of rating task (either meeting privacy expectations or complying with the privacy notice) throughout the 40 vignettes about tracking users online.

Sample

The respondents were recruited through Amazon Mechanical Turk (MTurk) for two surveys. There were 485 respondents and 19,400 vignettes for the privacy expectations survey and 488 respondents and 19,520 rated vignettes for the privacy notice survey. Table 1 contains the sample statistics across both survey samples.[2]

[2]Amazon Mechanical Turk is an online labor market in which requestors (academics) post jobs and the workers (respondents) choose jobs to complete. For a full description, see Mason and Suri (2012). For a discussion of how MTurk samples are more representative of the U.S. population than in-person convenience samples, see Berinsky, Huber, and Lenz (2012). For the external and internal validity of MTurk, see Horton, Rand, and Zeckhauser (2011). In a working paper, I specifically show how the empirical examination of privacy online with an MTurk sample favorably compares with a nationally representative sample with the factorial vignette survey methodology (for details, contact the author).

Table 1. Sample Statistics

	Meets Privacy Expectations	Conforms to Privacy Notice
Sample Size		
N (respondents)	485	488
N (vignettes)	19,400	19,520
Rating Task		
Average rating	–34.97	–25.11
SD of rating	38.55	44.89
Controls		
PrivacyImportant	71.93	75.23
TrustSites	5.88	4.05
Respondents		
Age	34.39	33.22
Male	57.1%	55.3%
Respondent R^2	.801	.806
Multilevel Analysis		
ICC	34.6%	27.9%

Independent Variables

Online Privacy Factors

The approach to privacy used here frames privacy as contextually defined by actors within a given community (Martin 2015; Nissenbaum 2004, 2009). As such, contextual factors such as the overall purpose of the website (context) as well as the frequency and tenure of the hypothetical person using the website were included across tracking situations. These contextual factors were not included in the analysis but provided realism in the vignette. The vignettes contained five categories of contextual factors used in the analysis:

- Information (4): Four types of information were systematically varied in the vignettes tracking users: (1) where users click on the page, (2) the search terms entered, (3) keywords on the page, and (4) general demographic information.
- Secondary use (3): How the data were reused or stored varied for vignettes. For tracked information, data can be (1) used for future targeted ads, (2) used for ads targeting friends, or (3) sold to a data broker/aggregator.
- Personalization (4): In addition, vignettes included tracked personalized information such as (1) consumer name, (2) references to friends, (3) location data, or (4) a unique computer identifier, none of which were disclosed by the person in the scenario.
- Storage (1): The length of time the data were stored varied as a continuous variable.
- Collection (2): The data collection actor varied between (1) a third-party advertiser or (2) the primary website.

The factors combine to produce 960 possible vignettes total (10 context × 1 tenure × 1 frequency × 4 information × 3 secondary use × 4 personalization × 2 collection × 1 storage) or 96 possible vignettes in the analysis without context included.

Control Variables

The respondents' age and gender were used in the regression analysis in addition to two control questions. Age has a positive correlation with a general concern for privacy and a negative correlation with specific judgments about meeting privacy expectations (Martin 2012a). In addition, research on the impact of gender on meeting privacy expectations and concerns about privacy is mixed, with female respondents judging online behavior as violating privacy expectations more often than male respondents (Martin 2011, 2012a).

Two individual beliefs or attitudes were captured to test the influence of individual-specific factors in making privacy judgments for H_2. First, trust has been found to be closely related to privacy (Pavlou 2011, p. 983); indeed, trust may be more important than privacy concerns as a predictor of behavior (Eastlick, Lotz, and Warrington 2006; Sultan and Rohm 2004; Van Slyke et al. 2006). The respondent was instructed to "tell us how much you agree with the statements below." Statements were rated on a sliding scale, with "strongly disagree" on the left and "strongly agree" on the right. The first rating task stated, "In general, I trust websites."

In addition, a general attitude toward privacy or a general belief that privacy is important varies across individuals, as outlined previously (Smith, Milberg, and Burke 1996; Xu et al. 2012). Accordingly, the second control rating task stated, "In general, I believe privacy is important."

Privacy Notice Prompt

For the privacy notice survey, a generic privacy notice was provided with the following instructions:

> First, the privacy statement below applies to all the hypothetical websites described in the study. This statement is illustrative of actual privacy policies. We are interested in how you think the vignettes conform to such a general privacy statement.… *You should read the statement with the time and attention that you would normally on a real website*.... THE PRIVACY STATEMENT — APPLIES TO ALL SURVEY WEBSITES.

This privacy notice was taken from an actual website with the name of the company replaced with "this website" throughout. The notice was purposefully chosen to be broad so that all scenarios would conform to it and was selected on the basis of consultation with a privacy law scholar specializing in privacy notices. For the full privacy notice provided to the respondents of the privacy notice survey, see the Web Appendix.

Dependent Variables: Privacy Rating Tasks.

For each vignette, respondents were given a rating task depending on the survey type, with the constant prompt "Tell us how much you agree with the statements below," using a sliding scale from –100 to 100, with –100 indicating "strongly disagree" and 100 indicating "strongly agree." For the privacy expectations survey, the respondents were given the statement "This website meets my privacy expectations." For the privacy notice surveys, the respondents were given the statement "This website conforms to the privacy notice." For respondents shown online tracking vignettes and asked to rate the degree to which the vignettes met their privacy expectations, a rating of 100 (–100) would strongly agree (strongly disagree) that the scenario meets privacy expectations. For respondents who were asked the degree to which the scenario conformed to the privacy notice provided in the beginning, a rating of 100 (–100) would strongly agree (strongly disagree) that the scenario conforms to the notice. Because the notice was chosen such that all hypothetical scenarios would conform to it, any rating less than 100 indicates that respondents perceive the action to not conform to the notice or mistakenly believe that the notice offers greater protection of their data than it actually does. The surveys measure (1) the degree to which the online tracking vignettes meet consumer privacy expectations as well as the factors and their relative importance to meeting privacy expectations and (2) the degree to which the vignettes conform to the privacy notice as well as the factors and their relative importance to conform to the notice.

Analysis

The data in this study were analyzed on two levels: the vignette-level factors and the respondent-level control variables. The model used in the analysis conceptualizes the ratings as a function of the contextual factors described in the vignette (ΣV_k) and the characteristics of the respondent (ΣR_h), as hypothesized previously. If I is the number of the respondents with Level 2 individual variables and J is the number of vignettes answered with Level 1 factor variables, the general equation is

$$(1)\ Y_{ij} = a_0 + s_k V_{jk} + \Sigma\gamma_h R_{hi} + u_i + e_j,$$

where Y_{ij} is the rating of vignette k by respondent i, V_{jk} is the kth factor of vignette j, R_{hi} is the hth characteristic of respondent i, β_0 is a constant term, s_k and γ_h are regression coefficients for k vignette factors and h respondent factors, u_i is a respondent-level residual (random effect), and e_j is a vignette-level residual.

Because the data can be modeled at two levels (the vignette level and the individual-respondent level), multilevel modeling was used to control for and measure individual variation in privacy judgments. Both ordinary least squares regressions and hierarchical regressions (xtmixed in Stata) were used to analyze the data to account for the possibility that the error terms were not equal across respondents.

Two quality checks were performed on the sample to ensure that the ratings could be used in the statistical analysis. First, the issue of respondent fatigue or respondent burden has been associated with factorial vignette surveys (Nock and Gutterbock 2010; i.e., when the judgments and associated errors cannot be assumed to be independent because of correlation within a single respondent's answers, whereas typically vignettes are pooled as independent). Respondent fatigue was not a factor for any models. The survey instrument was designed to capture the vignette sequence number (e.g., #1 or #2 vs. #37–#40) to analyze whether this affected the ratings or regression equations. These variables were used in the regression analysis and were not significant.

Second, previous use of factorial vignette surveys has shown a respondent learning curve, presumably from the novelty of the survey design (Martin 2012a). The variable signifying a low sequence number was significant for all samples; the regressions after dropping the first two vignettes did not change the results.

Results

Overall Privacy Judgments

H_1 predicts that the online tracking scenarios will be judged to conform to the privacy notice to a greater degree than judged to meet users' privacy expectations. For both the privacy expectations and privacy notice surveys, the general sample statistics were calculated as shown in Table 1. The mean degree to which the scenarios are judged to meet the respondent's privacy expectations (–34.97) is less than the degree to which the scenarios are judged to conform to the privacy notice (–25.11; t = 3.19, d.f. = 971, p = .00). These results support H_1's stance that online tracking scenarios will be judged to conform to the requirements of the privacy notice more than they will be judged to meet users' privacy expectations. Indeed, all vignettes fully conformed to the provided privacy notice by design and should have

been rated 100 for full conformance. However, respondents perceived the vignettes not to conform to a large degree (–25.11), suggesting that the respondents perceived the notice to be more protective of consumer data than it actually was.

Figure 2 graphs the difference between conforming to the privacy notice and meeting privacy expectations on the basis of the respondents' trust in websites. To mean-center the control variables, the respondents' score for their "trust-in-websites" rating was distributed into five groups for a trust quantile (labeled 0–4, with 0 = lowest 20% in the trust-in-websites score, and 4 = highest 20% in the trust-in-websites score). Figure 2 illustrates that as the respondents' trust in websites increases, the difference between the degree to which respondents judge scenarios to comply with the privacy notice and to meet their privacy expectations decreases. Respondents with greater trust in websites believe that their expectations are represented in the privacy notice.

In addition, the respondents' belief that privacy is important increases the difference between the degrees to which scenarios are judged to comply with the privacy notice and to meet their privacy expectations. As Figure 3 shows, as the belief that privacy is important increases, both the judgment about meeting privacy expectations and conforming to privacy notice decreases. Respondents with a greater belief that privacy is important have a greater gap between believing that the scenarios meet privacy expectations and that they conform to privacy notices.

The model statistics validate the use of multilevel modeling in Table 2. The intraclass coefficient (ICC) for the privacy expectations multilevel regressions is greater than for the privacy notice regressions, suggesting that a greater percentage of the variance in the rating task is attributable to respondents (rather than the vignette factors) for the privacy expectations rating (34.6%) than for the privacy notice rating (27.9%). Both ICC metrics indicate that the differences in judgments *across* respondents is large enough to justify using multilevel modeling rather than pooling the data and using linear regression.

Figure 2. Average Vignette Rating for Each Quantile of Trust-in-Websites Score

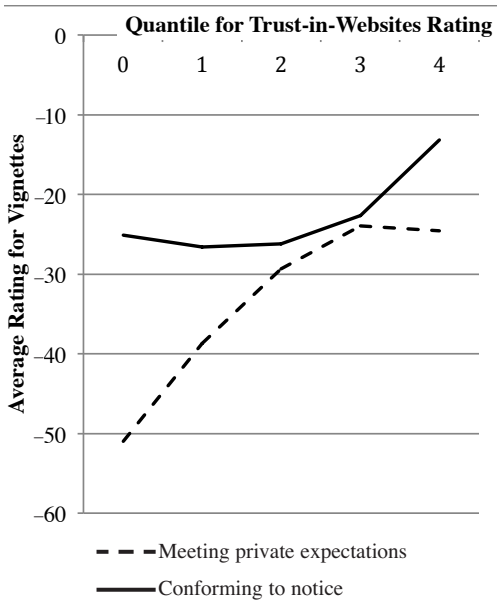
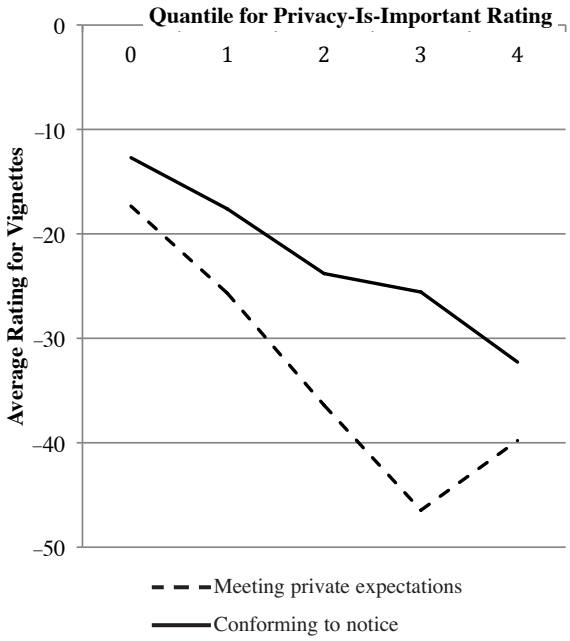


Figure 3. Average Vignette Rating for Each Quantile of Privacy-Is-Important Score



Factors Driving Judgments

H_2 predicts that the role of individual factors will be greater for privacy expectation judgments relative to judgments about conformity to privacy notice. To test H_2, the dependent variable for both the privacy expectations and privacy notice surveys was regressed on the contextual and individual factors. Table 2, Columns B and D, respectively, present the results.

Table 2 contains the relative importance of the individual factors to both types of judgments. The respondents' belief that privacy is important has statistically equivalent impact on privacy expectations ($\beta = -.215$, $p = .00$) and for the notice conformity judgment ($\beta = -.240$, $p = .00$; $\chi^2(14) = 2.45$, $p = .12$). However, the respondents' institutional trust in websites is significant for meeting privacy expectations ($\beta = .249$, $p = .00$) but not significant for judging whether scenarios conform to a privacy notice ($\beta = .033$, $p = .27$; $\chi^2(14) = 332.89$, $p = .00$).

In addition, the respondent-level control variables show a significant improvement for the privacy expectations model ($\Delta BIC_{B-A} = -72.8$; a lower number signifies a better fit), whereas the addition of the respondent-level control variables for the privacy notice model is not statistically significant because the Bayesian information criterion

Table 2. Multilevel Regression Results for Notice and Expectations Surveys

	Relative Importance in Making Judgment									
	Meeting Privacy Expectations				Conforming to Notice				Chow Test	
	Context Factors		+ Respondent Controls		Context Factors		+ Respondent Controls		Compare Coefficient	
	A		B		C		D		B versus D	
	β	*p*	β	*p*	β	*p*	β	*p*	χ^2	*p*
Type of Information										
ClickInfo	1.163	.13	1.167	.13	–.419	.63	–.408	.64	1.32	.25
KeywordInfo	1.154	.14	1.171	.13	–.400	.65	–.397	.65	2.68	.11
SearchInfo	2.564	.00	2.566	.00	.637	.46	.642	.46	3.28	.07
(null = DemographInfo)										
Personalization										
ComputerPersonalize	–8.185	.00	–8.183	.00	–8.048	.00	–8.054	.00	.00	.96
LocationPersonalize	–2.071	.01	–2.067	.01	–2.447	.01	–2.438	.01	.07	.79
NamePersonalize	–15.903	.00	–15.917	.00	–14.371	.00	–14.368	.00	.77	.38
(null = no personalization)										
Second Use										
FriendsSecondUse	–31.119	.00	–31.121	.00	–39.710	.00	–39.719	.00	47.87	.00
SellSecondUse	–44.886	.00	–44.891	.00	–57.442	.00	–57.444	.00	91.93	.00
(null = GeneralAd)										
Collecting Actor										
OutsideCollect	–3.669	.00	–3.662	.00	–3.751	.00	–3.750	.00	.06	.81
(null = PrimarySite)										
StorageMths	–.626	.00	–.627	.00	–.658	.00	–.658	.00		
Respondent Control Variables										
Male			7.871	.00			2.771	.33		
Age			–.057	.63			–.101	.44		
TrustSites			.249	.00			.033	.27	332.89	.00
PrivacyImportant			–.215	.00			–.240	.00	.06	.81
_cons	.105	.95	11.559	.03	18.217	.00	37.971	.00		
N	19,400				19,520					
ICC (Null)	34.6%				27.9%					
Deviance (Null)	202,116.6				208,807.8					
BIC (Null)	202,146.2				208,837.5					
Test Multilevel Versus Linear Regression										
sd(_cons)[a]	31.11		27.58		30.80		29.70			
ICC (model)[b]	40.5%		34.9%		34.5%		32.9%			
Test Current Versus Previous Model (Effect of Variates)										
Deviance	197,477.4		197,365.1		203,187.2		203,153.4			
Difference in deviance	–4,639.2		–112.32		–5,620.6		–33.8			
d.f.	10		4		10		4			
log ratio χ^2	4,639.2		112.3		5,620.7		33.8			
p	.00		.00		.00		.00			
BIC (model)	197,605.7		197,532.9		203,315.6		203,321.4			
Difference in BIC	–4,540.5		–72.8		–5,521.9		5.8			

[a]sd(_cons) = the standard deviation of the mean (_cons) for that equation across respondents. A larger standard deviation of the intercept suggests that the equation may shift on the basis of the respondent. It justifies the use of multilevel modeling.
[b]ICC = intraclass correlation coefficient; the percentage of variation attributable to the group variable (Level 2) or the individual. It justifies the use of multilevel modeling.

(BIC) increases with the additional variables in the model ($\Delta BIC_{D-C} = +5.8$). In addition, the difference-in-deviance chi-square test shows an improvement in the model by including respondent-level controls for both the privacy expectations ($\chi^2(4) = 112.3$, $p = .00$) and privacy notice ($\chi^2(4) = 33.8$, $p = .00$) regressions.

The results show mixed support for H_2. The role of institutional trust is significant to judgments about privacy expectations but not significant for judgments about conforming to privacy notices. However, the role of the privacy-is-important control is statistically equivalent across both judgments.

H_3 predicts that contextual factors (what information is collected, how information is used, who has access to the information, etc.) will affect judgments of whether users' privacy expectations are met more than judgments about complying with a general privacy notice. The results do not support H_3: the contextual factors driving judgments about privacy expectations are the same factors that drive judgments about conforming to privacy notices. That is, the factors that drove respondents to say that a vignette did not conform to the privacy notice were the same factors that drove respondents to say that a vignette did not meet their privacy expectations. Specifically, Table 2 includes a comparison of the coefficients for the factors driving meeting privacy expectations and conforming to a privacy notice.

Two contextual factors have statistically different impacts on meeting privacy expectations (Table 2, Column B) and conforming to a privacy notice (Table 2, Column D). The use of data to target friends to meet privacy expectations ($\beta = -31.12$, $p = .00$) significantly differs from the factor's importance in conforming to a notice ($\beta = -39.72$, $p = .00$; $\chi^2(1) = 47.87$, $p = .00$); and the importance of selling data to meet privacy expectations ($\beta = -44.89$, $p = .00$) significantly differs from the factor's importance in conforming to a notice ($\beta = -57.44$, $p = .00$; $\chi^2(1) = 91.93$, $p = .00$). However, both factors remain the top two drivers of both types of judgments, as Figure 4 illustrates. The other contextual factors included in Figure 4 are statistically equivalent. In addition, and most importantly, the top four drivers for both violating privacy expectations and not conforming to the privacy notice were selling the information to data aggregators, using information to target friends, and tracking the user's name or computer. In summary, the respondents judged that the scenarios did not conform to the notice when all scenarios did conform, and they projected the important factors of their privacy expectations onto the privacy notice.

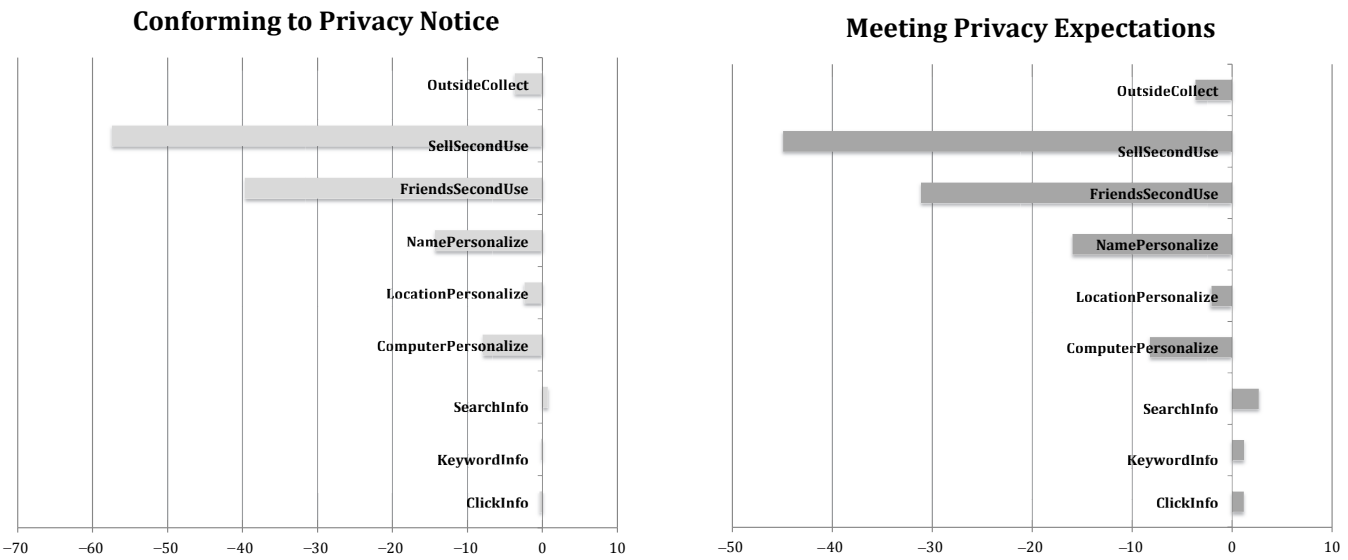
Discussion and Implications

Discussion of Results

This article analyzed the results of a study comparing users' privacy expectations with their judgments about conforming to privacy notices. Although much has been done to undermine the utility of privacy notices in assuaging privacy concerns online, this survey extends privacy scholarship by providing a direct comparison of privacy expectations and privacy notices. The results suggest that people's privacy expectations differ from conforming to privacy notices in important ways.

First, and perhaps not surprisingly, the respondents' perception of the privacy notice differed from the actual privacy notice. Respondents judged the privacy notice to be more protective of consumer data than the actual notice included in the survey. Specifically, the respondents on

Figure 4. Privacy Notice as Tabula Rasa: Contextual Factors Important to Meeting Privacy Expectations and Conforming to Privacy Notice



average disagreed that the vignettes conformed to the privacy notice, when all vignettes actually did conform by design.

Second, these results suggest that relying on privacy notices is inadequate to meet consumer privacy expectations. Respondents judged that the scenarios conformed to privacy notices but did not meet their privacy expectations. Notably, respondents with greater institutional trust in websites have a more realistic understanding of the privacy notice because their perception of the notice is closer to the actual notice. Furthermore, scenarios met expectations of privacy to a greater extent for respondents with greater institutional trust in websites. The finding provides renewed support of the important role of trust in online transactions.

Surprisingly, the factors that drove respondents to say that a vignette did not conform to the privacy notice were the same contextual factors that drove them to say that a vignette did not meet their privacy expectations. Although respondents were hypothesized to have privacy expectations that differed from the privacy notice, respondents perceived the notice to contain the same factors as their expectations.

In summary, the respondents judged that the scenarios did not conform to the notice when indeed all the scenarios did conform, and respondents projected the important factors to their privacy expectations onto the privacy notice. Privacy notices became a tabula rasa for users' privacy expectations. The results support the notion that privacy notices are insufficient to meet privacy expectations. This study found that users judged online scenarios to comply with the privacy notice to a greater degree than meeting their privacy expectations.

Public Policy and Practical Implications

With the current reliance on notice and choice as the basis for policy to address privacy expectations online, the findings have immediate implications for theory and practice. When privacy notices are used as the sole mechanism for respecting and protecting privacy online, the notice may be necessary but is not sufficient to meet privacy expectations. The key implications for public policy and practice are explained next.

Privacy Paradox

A continuing point of consternation for privacy research is the privacy paradox. This paradox is framed as the perceived inconsistency between people's stated concerns about privacy and their demonstrated or intended disclosure of information (Barnes 2006; John, Acquisti, and Loewenstein 2011; Norberg, Horne, and Horne 2007; Smith, Dinev, and Xu 2011). For example, in a review of privacy scholarship, Smith, Dinev, and Xu (2011, p. 993) summarize the privacy paradox thusly: "Despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances." According to the privacy paradox, consumers understand firms' privacy practices through the privacy statements but still choose to disclose their information. Consumers are then presumed to not actually care about privacy or to misunderstand the implications of their decisions (Acquisti and Grossklags 2005). The hypothetical paradox is based on the premise that notices serve as a clear communication device of the firm's online privacy practices.[3]

The findings here undercut the assumption that consumers accurately perceive the implications of disclosing information. Instead, consumers seem to perceive a highly protective environment when making sense of privacy notices. Blaming the act of disclosure on inappropriately valuing the decision presumes that consumers understand the decision. Rather than not identifying the risk or not finding the risk important, consumers actually perceive a safer environment than actually exists according to the current findings. In other words, the results indicate that people believe their privacy expectations are incorporated into the notice, thus suggesting that a stated concern about privacy and disclosure of information is not a paradoxical act.

Roles of Privacy Notice

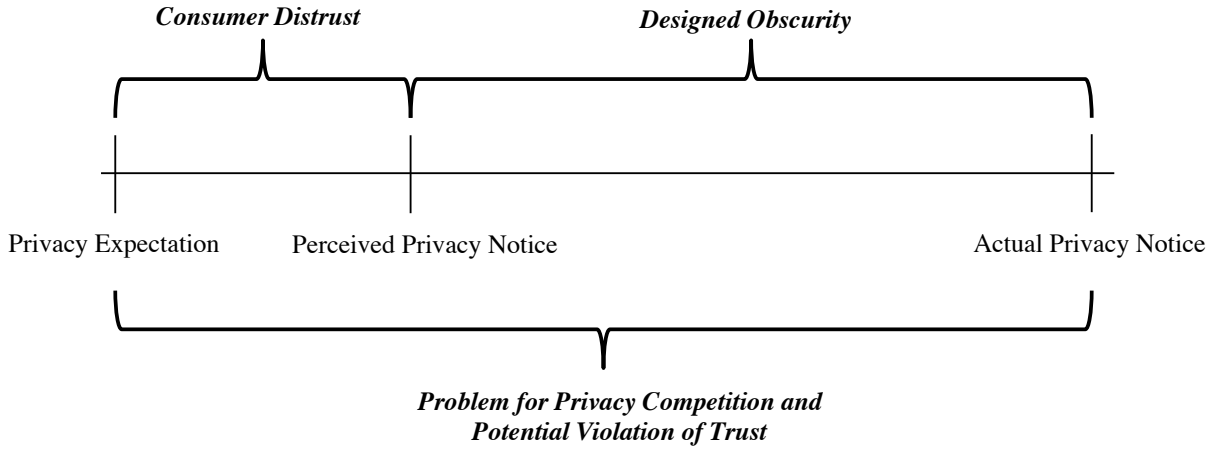
The finding that respondents perceive a notice that differs from the actual privacy notice also has implications regarding the utility of the notice as a communication device for firms. Firms understand how information will be used, stored, and disseminated after the consumer transaction, whereas the consumer does not. Privacy notices are designed to decrease the information asymmetries inherent in a firm's relationship with a consumer (Martin 2013). Yet the privacy notice fails in its role as a communication device in that the perceived privacy notice differed greatly from the actual notice, as Figure 5 illustrates.

One reason for the discrepancy between the actual and perceived privacy notice is the designed obscurity of the notice. In an exhaustive study of privacy notices, Marotta-Wurgler (2014) reports that firms use ill-defined terms such as "affiliates" or "third parties" to obscure the intended recipients of information. Also known as "weasel words" (McDonald et al. 2009), these purposefully ambiguous terms allow the privacy notice to be a blank slate—herein called a tabula rasa—for consumers' privacy expectations. To add to the designed obscurity, Marotta-Wurgler finds that 86% of studied contracts had broad "change of terms" clauses. Work in the area of misleading advertising and labeling may provide guidance on this issue, particularly Hastak and Mazis's (2011) conception of misleading due to semantic confusion or "deliberately confusing" language.

Instead, the privacy notice may be playing a larger role as a signal—more precisely, a false signal. Researchers have found that the mere presence of privacy statements can induce people to disclose personal information (Hui, Teo, and Lee 2007), yet the results reported here show that the privacy notice does not meet users' privacy expectations. Notably, Leon et al. (2012) find parallel results in a study of a privacy advertising icon, AdChoices. AdChoices was designed to provide only information about how an advertisement was placed on a website. Yet consumers mistakenly

[3]The privacy paradox is also based on the mistaken assumption that disclosing information is the same as relinquishing privacy expectations. People regularly disclose information while retaining privacy expectations (Hartzog 2011). Indeed, the findings of this survey show that people are quite nuanced about their expectations regarding the secondary use and third-party access to information.

Figure 5. Perceived Privacy Notices Versus Privacy Expectations



believed that the privacy icon blocked tracking and (mistakenly) trusted the icon to protect their information. Similarly, the findings herein suggest that the privacy notice is mistakenly believed to protect information more than the actual notice, and previous research has shown the presence of a privacy notice to induce sharing. The notice may provide to consumers a false signal of trustworthy behavior of the firm.

The difference between the actual and perceived privacy notice also undercuts notices' role as a means of facilitating competition over privacy practices (Beales 2003; Cranor 2012). The purpose of the notice within the role of facilitating competition should be to help consumers understand what information is collected, how it is used, and who has access to it. As currently operationalized in practice, notices are perhaps best suited for the "experienced user" (Cranor 2012) or regulators.

The current lack of choice in the online privacy marketplace could be a by-product of how the practices are communicated to consumers. Cranor et al. (2014) find little differentiation between firms with similar privacy practices around collecting and sharing information in their policies. All the financial firms in the study shared data for marketing and shared data on transactions and experience with affiliates. Perhaps firms offer bland, homogeneously worded policies because consumers cannot perceive any difference in privacy practices even if the firms do differentiate. In other words, some firms that regularly violate consumers' privacy norms could be seeking competitive parity by pushing to have all notices similarly constructed and obscure. Notably, this would suggest that firms with more consumer-friendly privacy practices would benefit from more clearly stating their practices or contributing to industry-wide "commonly accepted practices" (CAPs), as explored next.

Finally, the designed obscurity undermines the privacy notices' role as a contract (Marotta-Wurgler 2011). More work could be done to identify the CAPs, as suggested in a White House (2012) report, to provide a default for all firms. Firms would then only be required to explain how their practices deviate from the default. In addition, privacy notices' role as a contract would be strengthened with clear default rules for when a contract is unclear or silent on an issue (Marotta-Wurgler 2014), similar to other contract environments.

Alternatives to Privacy Statement

There are two alternatives to the lengthy privacy statements as effective notice, which are supported by the findings reported here. The gap between the written privacy notice provided in the sample and the perceived privacy notice judged by the respondents lends further support for machine-readable notification such as "P3P"—Platform for Privacy Preferences—which can be used in tools such as a privacy finder or privacy labels (Cranor 2012). Platform for Privacy Preferences, as originally designed, offered firms the ability to communicate their information management policies in P3P format so that browsers could read firms' policies and compare them with users' preferences. The notification would be provided at two levels: an easily read taxonomy with meaningful categories as well as a more detailed notice for experienced users, policy makers, or advocates (Cranor 2012).[4] Such an approach may shrink the gap in Figure 5 caused by designed obscurity.

Second, industry-level standards for CAPs (FTC 2010) would provide a minimum for the notice as a contract. Firms would be required to explain whether and how their practices differ from the CAPs, thereby removing some of the obscure details in the notice. In addition, the minimums would provide a proverbial backstop for the designed obscurity in the privacy notices, similar to other contracting environments:

[4]Although P3P remains attractive and has received renewed attention, the standard lacks enforcement, as Cranor summarizes on her website (see http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/).

when the notice is silent or obscure about a policy, the CAPs would provide guidance (Marotta-Wurgler 2014).[5]

The current design, involving lengthy and obscure privacy statements aimed toward consumers, imposes costs on consumers in the form of contact cost, as previous research has shown in the amount of time required to read the notice (McDonald and Cranor 2008). However, the current study suggests an additional reliance cost (identified generally in marketing by, e.g., Petty 2000), in that consumers engage with online firms under the mistaken impression that the privacy statement meets their privacy expectations. Redesigning the notice to streamline the consumer-targeted portion would reduce both contact and reliance costs for consumers.

Finally, rather than obscuring possibly privacy-violating behavior, firms could change their privacy practices. Recent research has suggested that the more invasive behavioral advertising that relies on personally identifiable tracked data is less effective than once believed. General ads perform better than highly targeted ads (Lambrecht and Tucker 2013), and social networking algorithms do better than highly targeted ads (Tucker 2014). Further research should address the incremental benefits of more invasive advertising and marketing efforts over alternatives such as contextual advertising or advertising on the basis of general demographic information. Such a tactic places more focus on the engineer or computer scientist to design privacy practices into the technology, as privacy experts (Mayer and Narayanan 2013) and public policy experts (Ohlhausen 2014a) have suggested.

[5]Commonly accepted practices as a default for notices is not the same as a government-imposed minimum requirement for managing information. Instead, firms would be required to disclose when and how they deviate from a default regarding (1) what information is collected, (2) who collects it, (3) how it is used, and (4) how long it is retained. For example, a default could be (1) only information volunteered by the user, which (2) remains within the purview of the primary firm (3) to improve services and (4) is retained for three months. I thank an anonymous reviewer for reinforcing this point.

Enforcement and Self-Regulation

The results indicate not only that the actual privacy notice does not meet users' privacy expectations but that the perceived notice is actually closer to users' expectations, as Figure 5 illustrates. Given these findings, the reaction of some firms to attempts to clarify privacy notices for consumers is understandable: some firms have little incentive to clearly articulate their current practices because the designed obscurity of their notice is perceived to meet consumers' privacy expectations. Indeed, such firms could require a large incentive to clarify their current privacy practices because their practices may not meet users' privacy expectations. This study explains why some firms may be reluctant to divulge the "gory detail" of privacy practices (Cranor 2012, p. 282) by clarifying notices: if firms were actually clear about privacy practices, consumers would share less information.

Conclusion

In comparing consumers' judgments about meeting privacy expectations with their judgments about conforming to privacy notices, this study directly supports both firms attempting to meet consumers' privacy expectations and public policy and the FTC's mission to protect consumer privacy, as *Journal of Public Policy & Marketing* has identified. Considering the importance of privacy notices in managing privacy online, more research should extend this study to shed light on how consumers understand notices and how consumers' perceptions of privacy notices map to their privacy expectations, if at all.

Appendix A. Sample Vignettes

A: Factors Common to All Vignettes

Factor	Dimensions	In Vignette (Context A/Context B/Context C ...)
Context[a]: The business of the primary organization; the underlying activity or purpose surrounding the exchange	Movies	Browsing movies/a movie guide/movies you look at/movie guide
	Social	Looking at/social networking/the content of your friends pages
	Medical	Researching on/medical research/the medical articles
	Retail	Shopping on/retail/the clothes you look at
	Search	Searching on/search engine/the search results
	News	Reading/a national news/the articles/national news
	Videos	Browsing videos on/a video sharing/the videos you look at/video sharing
	Travel	Searching on/travel/the flights and hotels you browse
	Banking	Working on/your banking statements/online banking/an online banking
	Payment	Checking your balance/your payment history/online payment services/an online payment services
Tenure: Time with organization	Months/years (continuous)	A week/less than a month/2 months/3 months/4 months/5 months/6 months/7 months
Frequency: Frequency of use	Hours per week (continuous)	Very frequently/frequently/occasionally/infrequently/rarely

Appendix A. Continued

B: Pilot II: Tracking Data

Factor	Dimensions	In Vignette
Information: Attributes; the type of information received or tracked by the primary organization	Role-based (looking – Web Bugs)	Where you clicked and looked on the page … is
	Top level	Search terms you have typed … are
	Contextual/content	Keywords on your current webpage … are
	Web travel	Your general online activity … is
Age: Time stored	Continuous months	XX months/years
Personalization	Name	Your name
	Location ID	Your location
	Demographic	Your age and gender
	Technology ID	A unique identifier for your computer
Collection: Who collects the information	Primary organization	The website … website
	Third-party tracking	An outside company's invisible tracking program … tracking company
Secondary use: What the collecting organization does with the information	Retargeting	Uses the information for future ads when you are online
	Data exchange	Sells the data in an online auction
	Social advertising	Uses the information for future ads targeting your friends and contacts.

Notes: Rating scales were as follows: Rating 1: For privacy expectations surveys: "This organization has met my privacy expectations (strongly disagree ... strongly agree). Rating 2: For privacy notice surveys: "This website confirms to the priacy notice (strongly disagree ... strongly agree).
[a]Context was chosen on the basis of the rankings from Google Ad Planner (http://www.google.com/adplanner/static/top1000/index.html#; accessed May 1, 2013) or by country (http://www.alexa.com/topsites/countries/US or http://www.alexa.com/topsites/countries).

Appendix B: Vignette Template

You are {Context_alt} {Context} website that you have used {Frequency} for about {Tenure}.
On the {Context_alt3} site, {Information} {Information_alt} collected by {Collection} and will be stored for {Age}. The data collected also includes {Personalization}.
The {Collection_alt} then {Second Use}.

Sample 1

You are shopping on a retail website that you have used once a day for about seven months.
On the retail site, your general online activity is collected by the website and will be stored for 6 months. The data collected also includes your demographic data.
The website then sells the data in an online auction.

Sample 2

You are working on an online banking website that you have used infrequently for about a week.
On the online banking site, where you clicked and looked on the page is collected by the website and will be stored for a month. The data collected also includes a unique identifier for your computer.
The website then uses the information for future ads targeting your friends and contacts

References

Acquisti, Alessandro and Jens Grossklags (2005), "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy*, 3 (1), 26–33.

——, Leslie K. John, and George Loewenstein (2013), "What Is Privacy Worth?" *Journal of Legal Studies*, 42 (2), 249–74.

—— and Hal R. Varian (2005), "Conditioning Prices on Purchase History," *Marketing Science*, 24 (3), 367–81.

Agarwal, Lalit, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani (2013), "Do Not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. New York: Association for Consumer Research, Article No. 8.

Angwin, Julia (2011), "Privacy Study: Top U.S. Websites Share Visitor Personal Data," *The Wall Street Journal*, (October 11), (accessed August 11, 2015), [available at http://blogs.wsj.com/digits/2011/10/11/privacy-study-top-u-s-websites-share-visitor-personal-data].

Bakos, Yannis, Florencia Marotta-Wurgler, and David R. Trossen (2014), "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts," *Journal of Legal Studies*, 43 (1), 1–35.

Barnes, Susan B. (2006), "A Privacy Paradox: Social Networking in the United States," *First Monday*, 11 (9), (accessed August 11, 2015), [available at http://firstmonday.org/article/view/1394/1312].

Barocas, Solon and Helen Nissenbaum (2009), "On Notice: The Trouble with Notice and Consent," *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, (October), 12–13.

Beales, J. Howard, III (2003), "The Federal Trade Commission's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," *Journal of Public Policy & Marketing*, 22 (Fall), 192–200.

——— and Jeffrey A. Eisenach (2014), "An Empirical Analysis of the Value of Information Sharing in the Market for Online Content," research report, Navigant Economics, (January), (accessed August 11, 2015), [available at https://www.aboutads.info/resource/fullvalueinfostudy.pdf].

——— and Timothy J Muris (2008), "Choice or Consequences: Protecting Privacy in Commercial Information," *University of Chicago Law Review*, 75 (1), 109–135.

Berinsky, Adam J., Gregory A. Huber, and Gabriel S. Lenz (2012), "Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk," *Political Analysis*, 20 (3), 351–68.

Boyles, Jan Lauren, Aaron Smith, and Mary Madden (2012), "Privacy and Data Management on Mobile Devices," Pew Research Center, (September 5), (accessed August 11, 2015), [available at http://www.pewinternet.org/Reports/2012/Mobile-Privacy.aspx].

Brunton, Finn and Helen Nissenbaum (2011), "Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation," *First Monday*, 16 (5), (accessed August 11, 2015), [available at http://firstmonday.org/article/view/3493/2955].

Calo, Ryan (2012), "Against Notice Skepticism in Privacy (and Elsewhere)," *Notre Dame Law Review*, 87 (3), 1027–72.

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 (2/3), 181–202.

Cranor, Lorrie Faith (2012), "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice," *Journal on Telecommunications & High Technology Law*, 10 (2), 273–308.

———, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au (2014), "Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies," working paper, (accessed August 11, 2015), [available at http://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=1794&context=fac_articles].

———, Kelly Idouchi, Pedro Giovanni Leon, Manya Sleeper, and Blase Ur (2013), "Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Practices," in *The Twelfth Workshop on the Economics of Information Security*, (accessed August 19, 2015), [available at http://weis2013.econinfosec.org/papers/CranorWEIS2013.pdf].

Culnan, Mary J. (1995), "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, 9 (2), 10–19.

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

——— and Pamela K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10 (1), 104–15.

——— and Robert J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59 (2), 323–42.

——— and Cynthia C. Williams (2009), "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly*, 33 (4), 673–87.

DMA Data-Driven Marketing Institute (2013), "The Value of Data: Consequences for Insight, Innovation, and Efficiency in the U.S. Economy: A Study Commissioned by DMA's Data-Driven Marketing Institute," press release, (October 14), Digital Marketing Association. http://ddminstitute.thedma.org/files/2013/10/DDMI-Summary-Analysis-Value-of-Data-Study.pdf.

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

Dwoskin, Elizabeth (2013), "Study: Digital Marketing Industry Worth $62 Billion," *The Wall Street Journal*, (October 14), (accessed August 11, 2015), [available at http://blogs.wsj.com/digits/2013/10/14/study-digital-marketing-industry-worth-62-billion].

Eastlick, Mary Ann, Sherry L. Lotz, and Patricia Warrington (2006), "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research*, 59 (8), 877–86.

FTC (2010), "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," preliminary FTC staff report, (December), (accessed August 11, 2015), [available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf].

——— (2012), "FTC's Privacy Report: Balancing Privacy and Innovation," (accessed August 11, 2015), [available at http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report].

——— (2014), "Data Brokers: A Call for Transparency and Accountability," research report, (May), (accessed August 11, 2015), [available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf].

Gabisch, Jason Aaron and George R. Milne (2014), "The Impact of Compensation on Information Ownership and Privacy Control," *Journal of Consumer Marketing*, 31 (1), 13–26.

Ganong, Lawrence H. and Marilyn Coleman (2006), "Multiple Segment Factorial Vignette Designs," *Journal of Marriage and Family*, 68 (2), 455–68.

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

Hagan, John, Gabrielle Ferrales, and Guillermina Jasso (2008), "How Law Rules: Torture, Terror, and the Normative Judgments of Iraqi Judges," *Law & Society Review*, 42 (3), 605–44.

Hartzog, Woodrow (2011), "Chain-Link Confidentiality," *Georgia Law Review*, 46, 657–704.

Hastak, Manoj and Michael B. Mazis (2011), "Deception by Implication: A Typology of Truthful but Misleading Advertising and Labeling Claims," *Journal of Public Policy & Marketing*, 30 (Fall), 157–67.

Hoffman, Donna L., Thomas P. Novak, and Marcos A. Peralta (1999), "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *The Information Society*, 15 (2), 129–39.

Horton, John J., David G. Rand, and Richard J. Zeckhauser (2011), "The Online Laboratory: Conducting Experiments in a Real Labor Market," *Experimental Economics*, 14 (3), 399–425.

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee (2007), "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, 31 (1), 19–33.

Hull, Gordon, Heather Richter Lipford, and Celine Latulipe (2011), "Contextual Gaps: Privacy Issues on Facebook," *Ethics and Information Technology*, 13 (4), 289–302.

Jasso, Guillermina (2006), "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research*, 34 (3), 334–423.

——— and Karl-Dieter Opp (1997), "Probing the Character of Norms: A Factorial Survey Analysis of the Norms of Political Action," *American Sociological Review*, 62 (6), 947–64.

John, Leslie K., Alessandro Acquisti, and George Loewenstein (2011), "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research*, 37 (5), 858–73.

Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor (2010), "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: Association for Computing Machinery, 1573–82.

Lambrecht, Anja and Catherine Tucker (2013), "When Does Retargeting Work? Information Specificity in Online Advertising," *Journal of Marketing Research*, 50 (October), 561–76.

Lanier, Clinton D. and Amit Saini (2008), "Understanding Consumer Privacy: A Review and Future Directions," *Academy of Marketing Science Review*, 12 (2), 1–45.

Leon, Pedro Giovanni, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, et al. (2012), "What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?" in *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society*. New York: Association for Computing Machinery, 19–30.

———, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh (2014), "Why People Are (Un)willing to Share Information with Online Advertisers," Workshop on Privacy in Electronic Society, (accessed August 11, 2015), [available http://www.andrew.cmu.edu/user/pgl/wpes2014oba.pdf].

———, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, et al. (2013), "What Matters to Users? Factors That Affect Users' Willingness to Share Information with Online Advertisers," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, Article No. 7. New York: Association for Computing Machinery.

Li, Han, Rathindra Sarathy, and Heng Xu (2010), "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems*, 51 (1), 62–71.

Marotta-Wurgler, Florencia (2011), "Some Realities of Online Contracting," *Supreme Court Economic Review*, 19 (1), 11–23.

——— (2014), "Does 'Notice and Choice' Disclosure Regulation Work? An Empirical Study of Privacy Policies," working paper, New York University School of Law.

Martin, Kirsten (2011), "TMI (Too Much Information): The Role of Friction and Familiarity in Disclosing Information," *Business and Professional Ethics Journal*, 30 (1/2), 1–32.

——— (2012a), "Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract," *Journal of Business Ethics*, 111 (4), 519–39.

——— (2012b), "Information Technology and Privacy: Conceptual Muddles or Privacy Vacuums?" *Ethics and Information Technology*, 14 (4), 267–84.

——— (2013), "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online," *First Monday*, 18 (12), (accessed August 11, 2015), [available at http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802].

——— (2015), "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics*, (accessed August 19, 2015), [available at http://link.springer.com/article/10.1007%2Fs10551-015-2565-9].

Mason, Winter and Siddharth Suri (2012), "Conducting Behavioral Research on Amazon's Mechanical Turk," *Behavior Research Methods*, 44 (1), 1–23.

Mayer, Jonathan (2014), "Tracking the Trackers: To Catch a History Thief," blog, The Center for Internet and Society at Stanford Law School, (July 19), (accessed November 2, 2014), [available at http://cyberlaw.stanford.edu/node/6695].

——— and Arvind Narayanan (2012), "Do Not Track: Universal Tracking Opt Out," (accessed August 11, 2015), [available at http://donottrack.us].

——— and ——— (2013), "Privacy Substitutes," *Stanford Law Review Online*, 66, 89–96.

McDonald, Aleecia M. and Lorrie Faith Cranor (2008), "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 4 (3), 540–65.

———, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor (2009), "A Comparative Study of Online Privacy Policies and Formats," in *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*. Berlin: Springer, 37–55.

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.

——— and Shalini Bahl (2010), "Are There Differences between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis," *Journal of Public Policy & Marketing*, 29 (Spring), 138–49.

———, ———, 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 (3), 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), 206–215.

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

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

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

Muris, Timothy J. (2001), "Protecting Consumers' Privacy: 2002 and Beyond," remarks at the FTC Privacy 2001 Conference, (October 4), (accessed August 11, 2015), [available at: https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond].

Nissenbaum, Helen (2004), "Privacy as Contextual Integrity," *Washington Law Review*, 79 (1), 119–58.

——— (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

——— (2011), "A Contextual Approach to Privacy Online," *Daedalus*, 140 (4), 32–48.

Nock, Steven and Thomas Guterbock (2010), "Survey Experiments," in *Handbook of Survey Research*, 2nd ed., Peter V. Marsden and James D. Wright, eds. Bingley, UK: Emerald Group Publishing.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs*, 41 (1), 100–126.

Ohlhausen, Maureen K. (2014a), "The Power of Data," remarks presented at the Privacy Principles in the Era of Massive Data Conference, Georgetown University McCourt School of Public Policy, (April 22), (accessed August 11, 2015), [available at http://www.ftc.gov/system/files/documents/public_statements/299801/140422georgetownbigdataprivacy.pdf].

——— (2014b), "Privacy Challenges and Opportunities: The Role of the Federal Trade Commission," *Journal of Public Policy & Marketing*, 33 (Spring), 4–9.

Pavlou, Paul A. (2011), "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?" *MIS Quarterly*, 35 (4), 977–88.

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

Petty, Ross D. (2000), "Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy," *Journal of Public Policy & Marketing*, 19 (Spring), 42–53.

——— (2003), "Wireless Advertising Messaging: Legal Analysis and Public Policy Issues," *Journal of Public Policy & Marketing*, 22 (Spring), 71–82.

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.

Pirson, Michael, Kirsten Martin, and Bidhan Parmar (2014), "Public Trust in Business and Its Determinants," in *Public Trust in Business*, Jared D. Harris, Brian Moriarty, and Andrew C. Wicks, eds. Cambridge, UK: Cambridge University Press, 116–52.

Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, et al. (2013), "Anonymity, Privacy, and Security Online," Pew Research Center, (September 5), (accessed August 11, 2015), [available at http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/].

Reidenberg, Joel R., Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, et al. (2014), "Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding," Fordham Law Legal Studies Research Paper No. 2418297, (accessed August 11, 2015), [available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418297].

Rossi, Peter Henry and Steven L. Nock (1982), *Measuring Social Judgments: The Factorial Survey Approach*. Beverly Hills, CA: Sage Publications.

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

Smith, H. Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, 35 (4), 989–1016.

———, Sandra J. Milberg, and Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, 20 (2), 167–96.

Solove, Daniel J. (2006), "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154 (3), 477–564.

Sultan, Fareena and Andrew J. Rohm (2004), "The Evolving Role of the Internet in Marketing Strategy: An Exploratory Study," *Journal of Interactive Marketing*, 18 (2), 6–19.

Tang, Zhulei, Yu (Jeffrey) Hu, and Michael D. Smith (2008), "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems*, 24 (4), 153–73.

Thurman, Quint C., Julie A. Lam, and Peter H. Rossi (1998), "Sorting Out the Cuckoo's Nest: A Factorial Survey Approach to the Study of Popular Conceptions of Mental Illness," *Sociological Quarterly*, 29 (4), 565–88.

Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti (2011), "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research*, 22 (2), 254–68.

Tucker, Catherine (2014), "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research*, 51 (October), 546–62.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy (2009), "Americans Reject Tailored Advertising and Three Activities That Enable It," (accessed August 17, 2015), [available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214].

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang (2012), "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Washington, DC: Association for Computing Machinery.

Urban, Jennifer M., Chris Jay Hoofnagle, and Su Li (2012), "Mobile Phones and Privacy," BCLT Research Paper Series, Center for the Study of Law & Society, University of California, Berkeley.

U.S. Government Accountability Office (2013), "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," research report, (September), (accessed August 11, 2015), [available at http://www.gao.gov/assets/660/658151.pdf].

Van Slyke, Craig, J.T. Shim, Richard Johnson, and James J. Jiang (2006), "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems*, 7 (1), (accessed September 29, 2015), [available at Available at: http://aisel.aisnet.org/jais/vol7/iss6/16].

Wallander, Lisa (2009), "25 Years of Factorial Surveys in Sociology: A Review," *Social Science Research*, 38 (3), 505–520.

Weiss, Debra Cassens (2010), "Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print," *ABA Journal*, (October 20), (accessed August 19, 2015), [available at http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print].

Westin, A. (1991), "Harris-Equifax Consumer Privacy Survey," technical report, Equifax Inc.

The White House (2012), "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," (February), (accessed August 13, 2015), [available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf].

——— (2014) "Big Data: Seizing Opportunities, Preserving Values," (May), (accessed August 13, 2015), [available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf].

Xu, Heng, Hock-Hai Teo, Bernard C.Y. Tan, and Ritu Agarwal (2012), "Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research*, 23 (4), 1342–63.

———, Cheng Zhang, Pan Shi, and Peijian Song (2009), "Exploring the Role of Overt vs. Covert Personalization Strategy in Privacy Calculus," *Academy of Management Proceedings*, 2009 (1), 1–6.