Privacy Notices as Tabula Rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online.[1]

Kirsten Martin, Ph.D.

George Washington University
School of Business

martink@gwu.edu

[1] This material is based upon 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 and in broadening the implications. In addition, the paper was improved through feedback from Mary Culnan, Howard Beales, Pedro Leon, and the attendees at the *Privacy Law Scholars Conference* (2013) as well as the *Academy of Management* annual meeting (2013). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Privacy Notices as Tabula Rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online.[2]

Abstract

Recent privacy scholarship has focused on the failure of adequate notice and consumer choice as a tool to address consumers' privacy expectations online. However, a direct examination of how complying with privacy notice is related to meeting privacy expectations online has not been performed. This paper reports the findings of two factorial vignette studies describing online consumer tracking, where respondents rated the degree online scenarios met consumers' privacy expectations or complied with a privacy notice. The results suggest respondents perceived the privacy notice as offering greater protections than the actual privacy notice. Perhaps most problematic, 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 over reliance on privacy notices. Considering the importance of privacy notices in managing privacy online, more work should extend this study to understand how consumers understand notices and how consumers' perceptions of privacy notices map to their privacy expectations – if at all.

Keywords: privacy, notice, privacy statements, business ethics, FIPPs

[2] This material is based upon 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 and in broadening the implications. In addition, the paper was improved through feedback from Mary Culnan, Howard Beales, Pedro Leon, and the attendees at the *Privacy Law Scholars Conference* (2013) as well as the *Academy of Management* annual meeting (2013). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Privacy Notices as Tabula Rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online.

Introduction

Firms increasingly track consumers online in retail and marketing efforts. The digital marketing industry is worth $62B (Dwoskin 2013) and Internet advertising, which reached $43B in 2013, is central to marketing strategies (Beales and Eisenach 2014). In order to make online marketing seamless and efficient, marketers "surreptitiously and inextricably" couple consumer tracking and marketing (Milne, Bahl, and Rohm 2008; see also Beales 2014; Beales 2012).[3] The scope of the digital marketing industry and online advertising in particular led Digital Marketing Association CEO 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 2014; DMA Data-Driven Marketing Institute 2014).

Yet, online privacy and consumer tracking *has* been the subject of recent public policy scrutiny across a broad array of government agencies (White House 2014; White House 2012; Federal Trade Commission 2012; Federal Trade Commission 2014; GAO 2013). Online privacy persists as a public policy issue since consumers remain concerned about online behavioral advertising and related tracking (McDonald and Cranor 2008; Leon et al. 2013; 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).

[3] And to fulfill marketers' needs for individualized information, data brokers collected 1.4B consumer transactions and 700B aggregated data elements in 2013 (Federal Trade Commission 2014).

Fair Information Practice principles (FIPs) has been the primary tool within public policy and practice to address privacy expectations online. While the 'notice-and-choice model' within FIPs has an alternative – the harm-based model (Beales and Muris 2008; Muris 2001) focusing on specific harms to the consumer – the FTC's recent guidance retains a focus on notice and choice (Ohlhausen 2014a). Notice and choice are seen as core to FIP in policy (Federal Trade Commission 2012; Federal Trade Commission 2010) and in practice (Sheehan 2005; Culnan and Armstrong 1999; Culnan and Williams 2009; Peslak 2005). In sum, 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 Ohlhausen, 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" (Ohlhausen 2014a; Ohlhausen 2014b). And, the reliance on notice-and-choice needs to reflect changes in technology and the marketplace (GAO 2013).

In fact, considerable agreement exists that notice and choice has failed to meet the privacy expectations of users online (Nissenbaum 2011), yet little has been done to specifically map out how compliance to a privacy notice meets privacy expectations, if at all. The goal of this paper is to determine whether and how judgments about privacy expectations online are related to judgments about compliance to 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 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 to privacy expectations.

In order 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 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 around privacy online (Ohlhausen 2014a). 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 (Ohlhausen 2014a). This study directly compares consumer preferences and expectations to how consumers perceive and understand privacy statements.

The results have implications to firms online as well as to privacy scholars in marketing management, public policy, and business ethics. The results show that a reliance on privacy notices to meet consumers' privacy expectations appears to provide a necessary, but not

sufficient, condition for meeting privacy expectations. When privacy notices are found to be insufficient in meeting privacy expectations, individuals have attempted to pull out of this information exchange and obfuscate their behavior using tools such as CacheCloak, donottrack.us (Mayer and Narayanan 2012), Bit Torrent Hydra, TOR, and TrackMeNot (Brunton and Nissenbaum 2011), which work to allow users to maintain their privacy expectations regardless of the privacy policy of a website. 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 over reliance on privacy notices.

Privacy Expectations and Privacy Notices

Privacy Expectations

Marketers and firms navigate an increasingly complicated maze of laws and regulations in regards to privacy. Firms must take into consideration laws such as COPPA, FCRA, HIPPA, and FERPA in addition to the ubiquitous Fair Information Practices primarily regulated by the FTC as mentioned above. And firms are assessed for their compliance with laws and regulations: e.g., their compliance with notice requirements of FIPs (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 if firms meet legal requirements, firms are judged if they meet privacy expectations of consumers. For example, Milne and Rohm (2000) shift from whether firms comply with FIP to examine how consumers *perceive* firms' compliance with FIP. The examination of consumers' privacy expectations in general (Phelps,

Nowak, and Ferrell 2000; Milne and Bahl 2010) and privacy expectations about specific technologies such as cookies (Miyazaki 2008) shift from focusing on how well a firm complies to rules and regulations to how consumers perceive the information practices of firms. Complicating the examination of privacy expectations, privacy expectations can vary by context, platform, and importantly here, 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 (2012)).

The examination of consumer privacy expectations, or consumers' preferences and desires about information privacy, have been recently defined as the social norms within particular information contexts becomes increasingly important in a self-regulating environment. For privacy expectations scholarship, the important metric for firms becomes defined by the *consumer* rather than regulators. And, in a self-regulating environment, meeting or not meeting consumer privacy expectations is important for firms to manage (Petty 2003) where the "congruency of [privacy] expectations can lead to higher levels of trust and a more munificent environment for all" (Milne and Bahl 2010, 138).

In addition, the close examination of consumer privacy expectations is important for firms to possibly influence privacy expectations through compensation, as found by Gabisch and Milne (2014) and to find a balance between invasive marketing tactics and privacy expectations of consumers (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.

While 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 what data is acceptable to collect, who can have access to it, whether the information should be kept confidential, and how the information can be shared and reused. Such privacy expectations are formed within a social contract (Martin 2012; Miyazaki 2008; Culnan 1995; Dunfee, Smith, and Ross Jr 1999; Milne and Gordon 1993), where 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 not be harmed, and to maintain trust.

Privacy Notices

The notice-and-choice model, also known as “awareness” and “control” (Milne 2000), relies upon 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 intention (Miyazaki and Fernandez 2000), as well as impacting both a willingness to disclose information (Phelps, Nowak, and Ferrell 2000) and a willingness 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, hard to read, and likely to be ignored (Martin 2013; Calo 2012; Nissenbaum 2011; Milne and Culnan 2004). Privacy notices may be literally unavailable to users (Ur et al. 2012) and unrealistically time intensive (McDonald and Cranor 2008). Privacy statements are found to be more difficult to understand than the average issue of the New York Times and require two

years of college education to comprehend (Sheehan 2005). In fact, 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, privacy statements are not improving and were found to decline in readability over time (Milne, Culnan, and Greene 2006). While scholarship has addressed *why* notices fail to address privacy expectations, this paper seeks to understand *how* notices fail to address consumer privacy expectations.

This study addresses the research question: how are judgments about privacy expectations online related to judgments about complying to privacy notices? For a given situation online, we can capture the degree to which the scenario meets users' privacy expectations of users and the degree to which the scenario is judged to comply with the privacy notice. As such, judgments about privacy expectations online can be compared to judgments about compliance to privacy notices along two dimensions: the judgments themselves as well as the factors 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 appropriateness and inappropriateness of the information transmitted within a particular context. In other words, individuals, 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 noted by Beales and Muris (2008), notice and choice may be <u>not necessary</u> for many of the most common

transactions such as when completing an ATM transaction (notice is not necessary), filing taxes (choice is not necessary), or credit reporting (neither notice nor choice is necessary). Individuals regularly give information without notice or choice and without believing that their privacy is being violated. In addition, notice and choice is 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 (Masnick 2010). Current academic research supports this notion: fewer than two out of 1000 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 individuals 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, where complying with privacy notices is akin to meeting privacy expectations of users. Particularly problematic for consumers is the lighter shaded area in Figure 1 where the notice is judged not sufficient to meet privacy expectations: practices conform to a privacy notice yet do not meet the privacy expectations of consumers.

INSERT FIGURE 1 ABOUT HERE

While Figure 1 is conceptualized as an equal chance of the privacy notice being insufficient or not necessary in meeting privacy expectations, in actuality firms regularly fail to meet the privacy expectations of users while conforming to privacy notices. In fact, privacy notices are purposefully designed to remain vague in order to allow for future tracking and targeting techniques and to accommodate future technological capabilities. The actors and transmission of information online are obscure with many indirect, third-party organizations

involved. In addition, policies change in order to incorporate technological upgrades or novel privacy measures and the policies become byzantine (Hull, Lipford, and Latulipe 2011).

We would therefore expect that online scenarios of tracking users would be judged as conforming to a privacy notice to a greater degree than judged as meeting privacy expectations.

> **Hypothesis 1:** *Scenarios of online tracking will be judged to comply with the privacy notice to a greater degree than judged to meet the privacy expectations of users.*

Factors that Impact Judgments.

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

Here we would expect similar results 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 individual to compare the scenario to 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 impacted by such individual factors. Where judgments about privacy expectations are

based, in part, on an individually-developed disposition, judgments about conforming to a privacy notice utilizes an external criterion – the privacy notice. In fact, notices are designed to ensure the privacy policies of a firm 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 to a privacy notice.

> **Hypothesis 2:** *Individual factors – such as an individual's institutional trust and general belief that privacy is important – will impact the meeting of privacy expectations of users 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 the novelty of technology (Martin 2012). Location-based privacy expectations would suggest that all activity 'online' carries similar privacy expectations. A more extreme version would suggest that the vary 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 privacy 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 2012; Xu et al. 2009), suggests rules for information flow take into account the purpose of the information exchange as well as risks and harms associated with sharing information. Rather than measuring privacy concerns and expectations as an attribute of individuals or the location of the exchange, contextual factors such as the type of information and the use of information, would impact privacy judgments.

Privacy notices, however, are viewed being less specific than contextual privacy expectations. In the analysis of privacy notices, research finds either silence on a particular issue, ambiguous language or broad 'change-of-terms' clauses allowing notices to allow almost every type information flow (Mcdonald et al. 2009; Cranor et al. 2014; Bakos, Marotta-Wurgler, and Trossen 2014; Marotta-Wurgler 2014). Even if individuals do read notices, organizations are limited in effectively communicating how information flows when online to consumers, and the notice statements are often not understood by consumers (Leon et al. 2012). Organizations with the best of intentions to notify users struggle to communicate complicated and changing policies which, 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).

In fact, the more specific the privacy policy, e.g., a policy that includes the type of information and how the information is used, the less agreement consumers have in interpreting the notice and the greater the notice is misunderstood by the average consumer (Reidenberg et al. 2014); respondents miss the nuances of the policy (Kelley et al. 2010). Where 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 quite broad and do not take into consideration the particular of the context.

> **Hypothesis 3:** *Contextual factors – such as what information is collected, how it is used, and who has access to the information – will impact judgments about meeting of privacy expectations of users more than judgments about compliance to a general privacy notice.*

Methods

As the goal of this research is to examine whether and how judgments about privacy expectations differ from judgments about privacy notice, the study utilized the factorial vignette survey methodology developed to investigate human judgments (Rossi and Nock 1982; Jasso 2006; Wallander 2009).

While established within sociology (Rossi and Nock 1982; Jasso, 2006; Wallander, 2009), the factorial vignette survey technique is less established within marketing or public policy. The methodology has been used in sociology to study such issues as political action (Jasso and Opp 1997), conceptions of mental illness (Thurman, Lam, and Rossi 1988), factors important to judgments of judges (Hagan, Ferrales, and Jasso 2008), and fairness of compensation (Jasso, 2006). In business ethics, the method has been used to study 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 (a) the factors used to form judgments, (b) the weight of each of these factors, and

(c) how different groups of the respondents agree on (a) and (b) (Nock and Guterbock 2010). These factors and their associated coefficients are referred to as the '*equations-inside-the-head*' (Jasso 2006) of respondents. By examining the equations-inside-the-head of respondents, 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 individuals require particulars of a situation 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 where norms should vary based on particular online situations. Second, the survey covers an area—privacy—which is fraught with respondent bias where 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 privacy factors and their relative importance of respondents. The respondents are not explicitly asked if selling information is appropriate; rather, respondents will rate a vignette wherein selling information is included among other factors and respondents are asked to rate that scenario. By asking respondents to rate multiple vignettes (40 vignettes), the respondent's factors and their relative importance are identified without directly asking for a ranking. Third, individuals often have difficulty articulating the factors and their relative importance that constitute their privacy expectations. As noted by the recent FTC report, traditional surveys are limited in their ability to measure privacy expectations of individuals (Federal Trade Commission 2010, fn 72).

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 was taking the survey. For each rated vignette, the associated rating, factor levels, and the vignette script was preserved as well as the vignette sequence number. The vignette formats are provided in the appendix 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 they received on tracking users online. Example vignettes are provided in the Appendix.

Sample

The respondents were recruited through Amazon Mechanical Turk for two surveys for a total of 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.[4]

INSERT TABLE 1 ABOUT HERE

Independent Variables

Online Privacy Factors.

The approach to privacy used here frames privacy as contextually defined by actors within a given community (Nissenbaum 2009; Nissenbaum 2004; Martin 2012). As such, contextual factors such as the overall purpose of the website (context) as well as the frequency

[4] Amazon Mechanical Turk (MTurk) is an online labor market where requestors, such as academics, post jobs and the workers, such as the respondents, choose jobs to complete. For a full description, see (Mason and Suri 2012), for how MTurk samples are more representative of the U.S. population than in-person convenience samples, see (Berinsky, Huber, and Lenz 2012), and for the external and internal validity of MTurk, see (Horton, Rand, and Zeckhauser 2011). Martin (2014) specifically shows how the empirical examination of privacy online with a MTurk sample favorably compares to a nationally representative sample with the factorial vignette survey methodology.

and tenure of the hypothetical user using the website were included across tracking situations. These contextual factors were not included in the analysis but provide 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: where users click on the page, the search terms entered, keywords on the page, and general demographic information.

Secondary Use (3): How the data was reused or stored varied for vignettes. For tracked information, data can be used for future targeted ads, used for ads targeting friends, or sold to a data broker/aggregator.

Personalization (4): In addition, vignettes included tracked personalized information, such as consumer name, references to friends, location data, or a unique computer identifier which were not disclosed by the individual in the scenario.

Storage (1): The length of time the data was stored varied as a continuous variable.

Collection (2): The data collection actor varied between a 3rd party advertiser or the primary website.

The factors combine to produce 960 possible vignettes total (10 Context x 1 Tenure x 1 Frequency x 4 Information x 3 Secondary Use x 4 Personalization x 2 Collection x 1 Storage) or 96 possible vignettes in the analysis without Context included in the analysis.

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 2012).

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 2012; Martin 2011).

Two individual beliefs or attitudes were captured to test the influence of individual-specific factors in making privacy judgments for Hypothesis 2. First, trust has been found to be closely related to privacy (Pavlou 2011, 983), where trust may be more important than privacy concerns as a predictor of behavior (Sultan and Rohm 2004; Eastlick, Lotz, and Warrington 2006; Van Slyke et al. 2006). The respondent was asked 'Tell us how much you agree with the statements below. On the sliding scale below, with a rating to the left being 'strongly disagree' to the right being 'strongly agree.' The rating task stated 'In general, I trust websites.'

In addition, a general attitude toward privacy or general belief that privacy is important varies across individuals as outlined above (Xu et al. 2012; Smith, Milberg, and Burke 1996). 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. The notice was chosen based on consultation with a privacy law

scholar specializing in privacy notices. See the appendix online for the full privacy notice provided to the respondents of the privacy notice survey.

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 the vignettes 'met their privacy expectations, a rating of +100 would be strongly agree that the scenario meets privacy expectations and a rating of -100 would be strongly disagree that the scenario meets privacy expectations. For respondents asked the degree to which the scenario conformed to a privacy notice provided in the beginning, a rating of +100 would be strongly agree that the scenarios conforms to the notice and a rating of -100 would be strongly disagree that the scenario conforms to the notice. Since the notice was chosen such that all hypothetical scenarios conform, any rating less than +100 indicates that respondents perceive the action to not conform to the notice or that the notice offers greater protection of their data.

The surveys measure the degree the online tracking vignettes meet consumer privacy expectations as well as the factors and their relative importance to meeting privacy expectations plus the degree the vignettes conform to notice with the factors and their relative importance to conform to the notice.

Analysis

The data in this study was analyzed on two levels: the vignette-level factors and the respondent-level control variables. The model used in the analysis and shown below 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 above. 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:

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

where Y_{ij} is the rating of vignette k by respondent i, V_{jk} is the k^{th} factor of vignette j, R_{hi} is the h^{th} 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.

As the data can be modeled at two levels – the vignettes and the individual respondents – multi-level modeling was used to control for and measure individual variation in privacy judgments. Both OLS regressions as well as hierarchical regressions (xtmixed in STATA) were used to analyze the data to account for the possibility that the error terms were not equal across individuals.

Two quality checks were performed on the sample to ensure 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 due to correlation within a single respondents' 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 in order to analyze if sequence number of the vignettes (e.g., #1 or 2 v. #37-40) impacted the ratings or regression equations. These variables were used in the regression analysis and were not significant.

Second, previous use of factorial vignette surveys found a respondents' *learning curve* – presumably from the novelty of the survey design (Martin 2012). 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

Hypothesis 1 predicts that the online tracking scenarios will be judged to conform to the privacy notice to a greater degree than judged to meet the privacy expectations of users.
For both the privacy expectations and privacy notice surveys, the general sample statistics were calculated as shown in Table 1. The mean degree that 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, $p = 0.00$). These results support hypothesis 1 that online tracking scenarios will be judged to conform to the requirements of the privacy notice more than judged to meet the privacy expectations of users. In fact, all vignettes did fully conform to the provided privacy notice by design, and should have been rated a +100 for full conformance. However, respondents perceived the vignettes to not conform to a large degree (-25.11) suggesting respondents perceived the notice to be more protective of consumer data than the actual notice provided.

The difference between conforming to privacy notice and meeting privacy expectations is graphed based on the respondents' trust in websites in Figure 2. To mean-center the control variables, the respondents' score for their 'trust-in-websites' rating was distributed into 5 groups for a trust quantile (labeled 0-4 with 4 = highest 20% in the trust-in-websites score; 0 = lowest 20% in the trust-in-websites score). Figure 2 illustrates that as the respondents' trust in websites increases, the difference between the degree scenarios are judged to comply with the privacy notice and the degree judged to meet the privacy expectations of respondents decreases. Respondents with greater trust in websites believe that their expectations are represented in the privacy notice.

Insert Figure 2 and 3 About Here

In addition, the respondents' belief that privacy is important increases the difference between the degree scenarios are judged to comply with the privacy notice and the degree judged to meet the privacy expectations of respondents. 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 the scenarios meet privacy expectations and conform to privacy notices.

The model statistics validate the use of multi level modeling in Table 2. The Intra-Class Coefficient (ICC) for the privacy expectations multi-level regressions is greater than privacy notice regressions suggesting a greater percentage of the variance in the rating task is attributable to individuals (rather than the vignette factors) for privacy expectations rating (34.6%) compared to the privacy notice rating (27.9%). Both ICC metrics suggest the differences in judgments

across individuals is large enough to justify using multi-level modeling rather than pooling the data and using linear regression.

Factors Driving Judgments

Hypothesis 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 hypothesis 2, the dependent variable for both the privacy expectations and privacy notice surveys were regressed on the contextual and individual factors. The results are in Table 2 in columns B and D respectively.

Insert Table 2 About Here

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 (β = -0.215, p = 0.00) and for the notice conformity judgment (β = -0.240, p = 0.00; $\chi^2(14) = 2.45$, p = 0.12). However, the respondents' institutional trust in websites is significant for meeting privacy expectations (β = 0.249, p = 0.00) but not significant for judging whether scenarios conform to a privacy notice (β = 0.033, p = 0.27; $\chi^2(14) = 332.89$, p = 0.00).

In addition, the respondent-level control variables is a significant improvement for the privacy expectations model (ΔBIC_{B-A} = -72.8, lower signifies a better fit) whereas the addition of the respondent-level control variables for the privacy notice model is not statistically significant as the BIC increases with the additional variables in the model (ΔBIC_{D-C} = +5.8). In addition, the difference in deviance χ^2 test shows an improvement in the model by including

respondent-level controls for both the privacy expectations ($\chi^2(4) = 112.3$, $p = 0.00$) and privacy notice ($\chi^2(4) = 33.8$, $p = 0.00$) regressions.

The results have mixed support for Hypothesis 2; the role of institutional trust is significant to judgments about privacy expectations but not significant for judgments about conforming to privacy notices supporting hypothesis 2. However the role of the privacy-is-important control is statistically equivalent across both judgments.

Hypothesis 3 predicts that contextual factors – such as what information is collected, how information is used, who has access to the information, etc. – will impact the meeting of privacy expectations of users more than judgments about complying to a general privacy notice. The results do not support hypothesis 3: *the contextual factors driving judgments about privacy expectations are the same factors that drive judgments about conforming to privacy notices*. Interestingly, the factors that drove respondents to say a vignette did not conform to the privacy notice were the same as the factors that drove respondents to say 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 (Column B in Table 2) and conforming to a privacy notice (Column D in Table 2). The use of data to target friends to meet privacy expectations ($\beta = -31.12$, $p = 0.00$) significantly differs from the factor's importance in conforming to a notice ($\beta = -39.72$, $p = 0.00$; $\chi^2(1) = 47.87$, $p = 0.00$); and the importance of selling data to meet privacy expectations ($\beta = -44.89$, $p = 0.00$) significantly differs from the factor's importance in conforming to a notice ($\beta = -57.44$, $p = 0.00$; $\chi^2(1) = 91.93$, $p = 0.00$). However, both factors remain the top two drivers of both types of judgments as best illustrated in Figure 4. 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 name or computer of the user as shown in Figure 4.

Insert Figure 4 About Here

In sum, the respondents judged that the scenarios did not conform to the notice when all scenarios did conform, and respondents projected the important factors to their privacy expectations onto the privacy notice.

Discussion And Implications

Discussion of Results

This paper analyzed the results of a study comparing the privacy expectations of users to their judgments about conforming to privacy notices. While 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 the 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 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 while still not meeting the privacy expectations of users. Interestingly, respondents with greater institutional trust in websites have a more realistic understanding of the privacy notice since the perceived notice is closer to the actual notice. Further, scenarios met expectations of privacy to a greater extent for respondents with higher 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 a vignette did not conform to the privacy notice were the same contextual factors that drove respondents to say a vignette did not meet their privacy expectations. While respondents were hypothesized to have privacy expectations that differ from the privacy notice, respondents perceived the notice to contain the same factors as their expectations.

In sum, the respondents judged that the scenarios did not conform to the notice when in fact 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 to theory and practice. When privacy notices are used as the sole mechanism to respecting and protecting privacy online, the

notice may be necessary *but not sufficient* to meet privacy expectations. The key implications for public policy and practice are explained below.

Privacy Paradox.

A continuing point of consternation for privacy research is the privacy paradox. This paradox is framed as the perceived inconsistency between an individuals' stated concerns about privacy and their demonstrated or intended disclosure of information (Barnes 2006; Smith, Dinev, and Xu 2011; John, Acquisti, and Loewenstein 2011; Norberg, Horne, and Horne 2007). For example, in a review of privacy scholarship, Smith et al. summarize the privacy paradox as "despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances" (Smith, Dinev, and Xu 2011). According to the privacy paradox, consumers understand the privacy practices of the firms through privacy statements but still disclose their information. Consumers are then presumed to not actually care about privacy or to not understand 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 privacy practices of the online firm.[5]

The findings here undercut the assumption that consumers accurately perceive the implications of disclosing information. Instead, consumers appear 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

[5] The privacy paradox is also based on the mistaken assumption that disclosing information is the same as relinquishing privacy expectations. Individuals regularly disclose information while retaining privacy expectations (Hartzog 2011). In fact, the findings of this survey show that individuals are quite nuanced about their expectations around the secondary use and third party access to information.

environment than exists according to the findings here. In other words, the results here suggest *individuals 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 to 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 where the consumer does not. Privacy notices are designed to decrease the information asymmetries inherent in a firms' 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 illustrated in Figure 5.

INSERT FIGURE 5 ABOUT HERE

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, Florencia Marotta-Wurgler notes that firms use ill-defined terms such as "affiliates" or "3rd parties" in order to obscure the intended recipients of information (Marotta-Wurgler 2014). Also known as "weasel words" (Mcdonald et al. 2009), these purposefully ambiguous terms allow the privacy notice to be a blank slate – here called a *tabula rasa* – for consumers' privacy expectations. To add to the designed obscurity, Moratta-Wurgler found that 86% of studied contracts had broad 'change of terms' clauses (Marotta-Wurgler 2014). Work in the area of misleading advertising and labeling

may provide guidance – particularly Hastak and Mazis (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 individuals to disclose personal information (Hui, Teo, and Lee 2007), yet the results reported here found that the privacy notice does not meet the privacy expectations of users. Interestingly, Leon et al. (Leon et al. 2012) found parallel results in a study of a privacy advertising icon, AdChoices. AdChoices was designed to only provide information about how an advertisement was placed on a website. Yet, consumers mistakenly believed that the privacy icon blocked tracking and (mistakenly) trusted the icon to protect their information. Similarly, the findings here 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 a false signal of trustworthy behavior of the firm for consumers.

The difference between the actual and perceived privacy notice also undercuts notices' role as a means of facilitating competition over privacy practices (Cranor 2012; Beales 2003). The purpose of the notice within the role of facilitating competition should be to help consumers understand what information is collected, how information is used, and who else has access to the information. 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 byproduct of how the practices are communicated to consumers. Cranor, Leon, and Ur (2014) found 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, homogenously worded policies because consumers cannot perceive any difference in privacy practices *even if the firms do differentiate.* In other words, some firms – who regularly violate the privacy norms of consumers – could be seeking competitive parity by pushing to have all notices similarly constructed and obscure. Interestingly, this would suggest that firms with more consumer friendly privacy practices would benefit from more clearly stating their practices or contribute to industry-wide 'commonly accepted practices' (CAP) as explored below.

Finally, the designed obscurity undermines the privacy notices' role as a contract (Marotta-Wurgler 2011). More work could be done to identify the commonly accepted practices, as suggested in a White House report (2012), in order 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 may find support from 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). P3P, 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 to users'

preferences. The notification would be provided at two levels: one is an easily read taxonomy with meaningful categories as well as a more detailed notice for experienced users, policy makers, or advocates(Cranor 2012).[6] Such an approach may shrink the gap in Figure 5 caused by designed obscurity.

Second, industry-level standards for commonly accepted practices (Federal Trade Commission 2010)would provide a minimum for the notice as a contract. Firms would be required to explain whether an how their practices differed from the commonly accepted practices 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: when the notice is silent or obscure about a policy, the commonly accepted practices would provide guidance (Marotta-Wurgler 2014).[7]

The current design – lengthy and obscure privacy statements aimed towards consumers – imposes costs on consumer in the form of contact cost as has been shown previously in the mount of time required to read the notice (McDonald and Cranor 2008). However, the study here suggests an additional *reliance* cost, e.g., identified generally in marketing by Petty (2000), in that consumers engage with online firms under the mistaken impression that their privacy expectations are being met in the privacy statement. 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

[6] While P3P remains attractive and constantly received renewed attention, the standard lacked enforcement as summarized by Prof. Cranor here http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/.

[7] CAP 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 around (1) what information is collected, (2) who collects, (3) how information is used, and (4) how long information is retained. For example, a default could be (1) only information volunteered by the user, (2) remains within the purview of the primary firm, (3) in order to improve services, and (4) retained for 3 months. I wish to thank an anonymous reviewer for reinforcing this point.

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). Privacy law scholar Paul Ohm notes that not enough research has been done around the incremental benefits of more invasive advertising and marketing efforts over alternatives such as contextual advertising or advertising based on general demographic information (2014). Such a tactic places more focus on the engineer or computer scientist to design privacy practices into the technology as has been suggest by privacy experts (Mayer and Narayanan 2013) and public policy experts (Ohlhausen 2014b).

Enforcement and Self-Regulation.

The results suggest that the actual privacy notice does not meet privacy expectations of users and that the perceived notice is actually closer to the expectations of the user as in Figure 5. Given the findings here, 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 as the designed obscurity of their notice is perceived to meet the consumer's privacy expectations. Clarifying current privacy practices could need a large incentive for some firms since their current practices may not meet the privacy expectations of users. This study explains why some firms may be reluctant to divulge the "gory detail" of privacy practices (Cranor 2012, 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 meeting the privacy expectations of consumers and public policy and the FTC's mission to protect consumer privacy – as has been identified in the Journal of Public Policy and Marketing. Considering the importance of privacy notices in managing privacy online, more work should extend this study to understand how consumers understand notices and how consumers' perceptions of privacy notices map to their privacy expectations – if at all.

REFERENCES

Acquisti, Alessandro, and Jens Grossklags. 2005. “Privacy and Rationality in Individual Decision Making.” *IEEE Security & Privacy* 2: 24–30.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. “What Is Privacy Worth?” *The Journal of Legal Studies* 42 (2): 249–74. doi:10.1086/671754.

Acquisti, Alessandro, and Hal R. Varian. 2005. “Conditioning Prices on Purchase History.” *Marketing Science* 24 (3): 367–81. doi:10.1287/mksc.1040.0103.

Agarwal, Lalit, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. 2013. “Do Not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising.” In , 8. ACM.

Angwin, Julia. 2011. “Privacy Study: Top U.S. Websites Share Visitor Personal Data.” *Wall Street Journal*. 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.” *The 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).

Barocas, Solon, and Helen Nissenbaum. 2009. “On Notice: The Trouble with Notice and Consent.” In , 12–13.

Beales, Howard, and Jeffrey A Eisenach. 2014. “An Empirical Analysis of the Value of Information Sharing in the Market for Online Content.” *Available at SSRN 2421405*.

Beales III, J Howard. 2003. “The Federal Trade Commission’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection.” *Journal of Public Policy & Marketing* 22 (2): 192–200.

Beales, J Howard, and Timothy J Muris. 2008. “Choice or Consequences: Protecting Privacy in Commercial Information.” *The University of Chicago Law Review*, 109–35.

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*. Washington, D.C.: Pew Internet & American Life Project. 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).

Calo, Ryan. 2012. “Against Notice Skepticism in Privacy (and Elsewhere).” *Notre Dame Law Review* 87.

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. doi:10.1007/s10799-005-5879-y.

Cranor, Lorrie Faith. 2012. “Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice.” *J. on Telecomm. & High Tech. L.* 10: 273.

Cranor, Lorrie Faith, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. 2014. “Are They Worth Reading? An In-- depth Analysis of Online Advertising Companies’ Privacy Policies.” *An In-Depth Analysis of Online Advertising Companies’ Privacy Policies (March 31, 2014)*.

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 (1): 20–26.

Culnan, Mary J., and Pamela K. Armstrong. 1999. “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10 (1): 104–15. doi:10.1287/orsc.10.1.104.

Culnan, Mary J., and Robert J. Bies. 2003. “Consumer Privacy: Balancing Economic and Justice Considerations.” *Journal of Social Issues* 59 (2): 323–42. doi:10.1111/1540-4560.00067.

Culnan, Mary J, and Cynthia C Williams. 2009. “How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches.” *Management Information Systems Quarterly* 33 (4): 6.

DMA Data-Driven Marketing Institute. 2014. *The Value of Data: Consequences for Insight, Innovation, and Efficience in the U.S. Economy.* 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.” *The Journal of Marketing*, 14–32.

Dwoskin, Elizabeth. 2014. “Study: Digitial Marketing Industry Worth $62 Billion.,” October 14. 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.

Federal Trade Commission. 2010. *Protecting Consumer Privacy in an Era of Rapid Change.* FTC. 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*. FTC. http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report.

———. 2014. *Data Brokers: A Call for Transparency and Accountability*. FTC. 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.

GAO. 2013. *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*. http://www.gao.gov/assets/660/658151.pdf.

Goodwin, Cathy. 1991. “Privacy: Recognition of a Consumer Right.” *Journal of Public Policy & Marketing*, 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.” *Ga. L. Rev.* 46: 657.

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 (2): 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*, 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.

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 , 1573–82. ACM.

Lambrecht, Anja, and Catherine Tucker. 2013. “When Does Retargeting Work? Information Specificity in Online Advertising.” *Journal of Marketing Research* 50 (5): 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, and Guzi Xu. 2012. “What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?” In , 19–30. ACM.

Leon, Pedro Giovanni, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. “Why People Are (Un) Willing to Share Information with Online Advertisers.”

Leon, Pedro Giovanni, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. “What Matters to Users?: Factors That Affect Users’ Willingness to Share Information with Online Advertisers.” In , 7. ACM.

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.

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

Martin, Kirsten. 2011. “TMI (Too Much Information).” *Business and Professional Ethics Journal* 30 (1/2): 1–32.

———. 2012. “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).

Martin, Kirsten E. 2012. “Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract.” *Journal of Business Ethics* 111 (4): 519–39. doi:10.1007/s10551-012-1215-8.

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: Where Everybody Knows Your Username*. Accessed November 2. http://cyberlaw.stanford.edu/node/6740.

Mayer, Jonathan, and Arvind Narayanan. 2012. *Donottrack*. http://donottrack.us.

———. 2013. “Privacy Substitutes.” *Stanford Law Review Online* 66: 89.

McDonald, Aleecia M, and Lorrie Faith Cranor. 2008. “Cost of Reading Privacy Policies, the.” *ISJLP* 4: 543.

Mcdonald, Aleecia M, Robert W Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. “A Comparative Study of Online Privacy Policies and Formats.” In , 37–55. Springer.

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 (1): 1–6.

Milne, George R, 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 (1): 138–49.

Milne, George R, Shalini Bahl, and Andrew Rohm. 2008. “Toward a Framework for Assessing Covert Marketing Practices.” *Journal of Public Policy & Marketing* 27 (1): 57–62.

Milne, George R, 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.

Milne, George R, Mary J Culnan, and Henry Greene. 2006. “A Longitudinal Assessment of Online Privacy Notice Readability.” *Journal of Public Policy & Marketing* 25 (2): 238–49.

Milne, George R., and Mary Ellen Gordon. 1993. “Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework.” *Journal of Public Policy & Marketing* 12 (2): 206–15.

Milne, George R, 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 (2): 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 (1): 19–33.

Miyazaki, Anthony D, and Ana Fernandez. 2000. “Internet Privacy and Security: An Examination of Online Retailer Disclosures.” *Journal of Public Policy & Marketing* 19 (1): 54–61.

Muris, Timothy J. 2001. *Protecting Consumers’ Privacy: 2002 and Beyond*. US FTC.

Nissenbaum, Helen. 2004. “Privacy as Contextual Integrity.” *Wash. L. Rev.* 79: 119.

———. 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*, edited by Peter V Marsden and James D Wright. 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. “Privacy Challenges and Opportunities: The Role of the Federal Trade Commission.” *Journal of Public Policy & Marketing* 33 (1): 4–9.

———. 2014b. “The Power of Data.” Remarks presented at the Privacy Principles in the Era of Massive Data, Georgetown University McCourt School of Public Policy, April 22. http://www.ftc.gov/system/files/documents/public_statements/299801/140422georgetownbigdataprivacy.pdf.

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 (1): 42–53.

———. 2003. “Wireless Advertising Messaging: Legal Analysis and Public Policy Issues.” *Journal of Public Policy & Marketing* 22 (1): 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 (1): 27–41.

Pirson, Michael, Kirsten Martin, and Bidhan Parmar. 2014. “Public Trust in Business and Its Determinents.” In *Public Trust in Business*, edited by Jared D Harris, Brian Moriarty, and Andrew C Wicks, 116–52. Cambridge University Press.

Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. “Anonymity, Privacy, and Security Online.” *Pew Research Center*.

Reidenberg, Joel R, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia M McDonald, Thomas B Norton, and Rohan Ramanath. 2014. “Disagreeable Privacy Policies: Mismatches between Meaning and Users’ Understanding.”

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

Sheehan, Kim Bartel. 2005. “In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites.” *Journal of Public Policy & Marketing* 24 (2): 273–83.

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

Smith, H. Jeff, 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*, 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.

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*.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. “Americans Reject Tailored Advertising and Three Activities That Enable It.” *Available at SSRN 1478214*.

Urban, Jennifer M., Chris Jay Hoofnagle, and Su Li. 2012. *Mobile Phones and Privacy*. BCLT Research Paper Series. Berkeley, CA: University of California at Berkeley - Center for the Study of Law and Society. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. “Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising.” In , 4. ACM.

Van Slyke, Craig, JT 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): 16.

Wallander, Lisa. 2009. “25 Years of Factorial Surveys in Sociology: A Review.” *Social Science Research* 38 (3): 505–20.

Westin, A. 1991. *Harris Louis & Associates. Harris-Equifax Consumer Privacy Survey*. Tech. rep, Conducted for Equifax Inc. 1,255 adults of the US public.

White House. 2012. *Consumer Data Privacy in a Networked World*. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

———. 2014. “Big Data: Seizing Opportunities, Preserving Values.” http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Xu, Heng, Hock-Hai Teo, Bernard CY 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.

Xu, Heng, 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. doi:10.5465/AMBPP.2009.44249857.

Tables And Figures

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
St Dev 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 R2	0.801	0.806
Multi Level Analysis		
ICC	34.6%	27.9%

Table 2: Multi-Level Regression Results for Notice and Expectations Surveys

	Relative Importance in Making Judgment								Chow Test Compare Coef	
	Mtg Privacy Expectations				Conforming to Notice					
	Context Factors		+ Respondent Controls		Context Factors		+ Respondent Controls			
	A		B		C		D		B v. D	
	β	p	β	p	β	p	β	p	Chi 2	p
Type of Information										
ClickInfo	1.163	0.13	1.167	0.13	-0.419	0.63	-0.408	0.64	1.32	0.25
KeywordInfo	1.154	0.14	1.171	0.13	-0.400	0.65	-0.397	0.65	2.68	0.11
SearchInfo	2.564	0.00	2.566	0.00	0.637	0.46	0.642	0.46	3.28	0.07
(null = DemographInfo)										
Personalization										
ComputerPersonalize	-8.185	0.00	-8.183	0.00	-8.048	0.00	-8.054	0.00	0.00	0.96
LocationPersonalize	-2.071	0.01	-2.067	0.01	-2.447	0.01	-2.438	0.01	0.07	0.79
NamePersonalize	-15.903	0.00	-15.917	0.00	-14.371	0.00	-14.368	0.00	0.77	0.38
(null = no personalization)										
Second Use										
FriendsSecondUse	-31.119	0.00	-31.121	0.00	-39.710	0.00	-39.719	0.00	*47.87*	*0.00*
SellSecondUse	-44.886	0.00	-44.891	0.00	-57.442	0.00	-57.444	0.00	*91.93*	*0.00*
(null = GeneralAd)										
Collecting Actor										
OutsideCollect	-3.669	0.00	-3.662	0.00	-3.751	0.00	-3.750	0.00	0.06	0.81
(null = PrimarySite)										
StorageMths	-0.626	0.00	-0.627	0.00	-0.658	0.00	-0.658	0.00		
Respondent Control Variables										
Male			7.871	0.00			2.771	0.33		
Age			-0.057	0.63			-0.101	0.44		
TrustSites			0.249	0.00			0.033	0.27	*332.89*	*0.00*
PrivacyImportant			-0.215	0.00			-0.240	0.00	0.06	0.81
_cons	0.105	0.95	11.559	0.03	18.217	0.00	37.971	0.00		
N	19,400				19,520					
ICC (Null)	34.6%				27.9%					
Deviance (Null)	202116.6				208807.8					
BIC (Null)	202146.2				208837.5					
Test Multi-Level v. Linear Regression										
sd(_cons)	31.11		27.58		30.80		29.70			
ICC (model)	40.5%		34.9%		34.5%		32.9%			
Test Current v. Previous Model (Effect of Variates)										
Deviance	197477.4		197365.1		203187.2		203153.4			
Difference in Deviance	-4639.2		-112.32		-5620.6		-33.8			
df	10		4		10		4			
log ratio X2	4639.2		112.3		5620.7		33.8			
p	0.00		0.00		0.00		0.00			
BIC (Model)	197605.7		197532.9		203315.6		203321.4			
Difference in BIC	-4540.5		-72.8		-5521.9		5.8			

**Notes for Table 2:

1. *ICC = Intraclass Correlation Coefficient = % of variation attributable to the group variable (Level 2) or the individual here. Justifies the use of multi-level modeling.*
2. *sd(_cons) = the st dev of the mean (_cons) for that equation across individuals. Larger standard deviation of the intercept suggests the equation may <u>shift</u> based on the individual. Justifies the use of multi-level modeling.*

Figure 1: Relationship between meeting privacy expectations and conforming to privacy notice

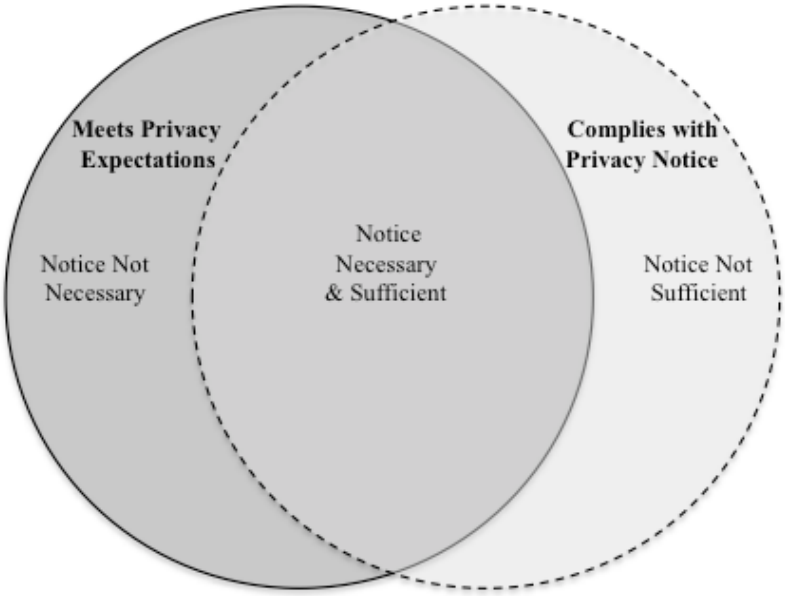


Figure 2: Average vignette rating for each quantile of trust-in-websites score.

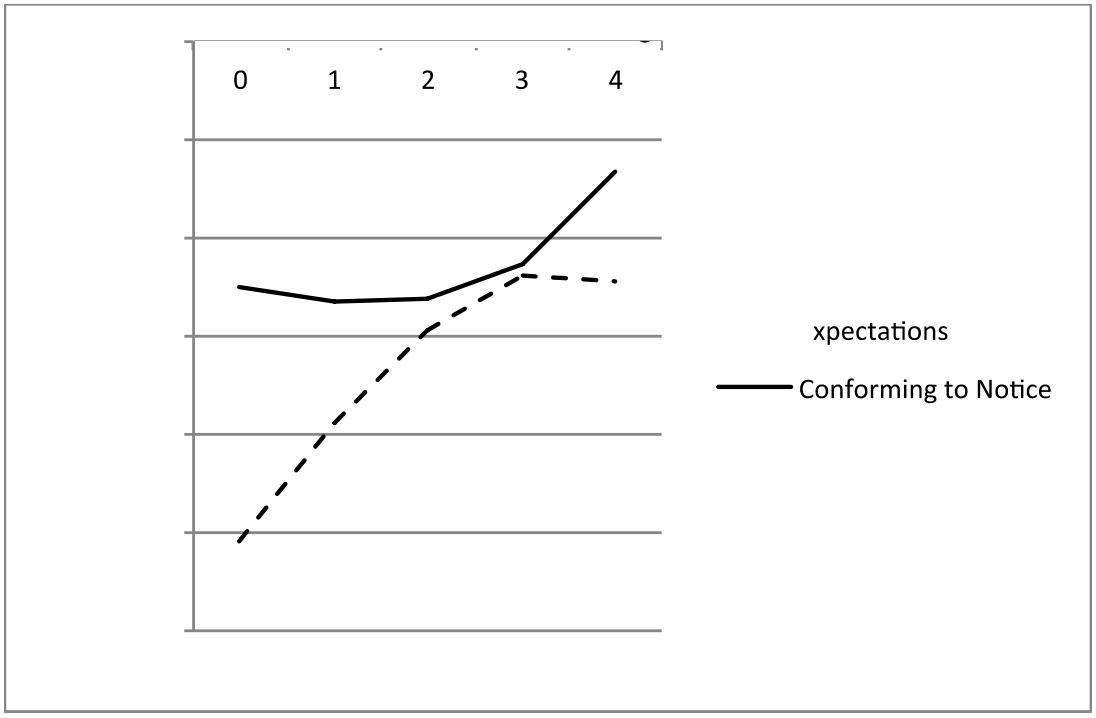


Figure 3: Average vignette rating for each quantile of privacy-is-important score.

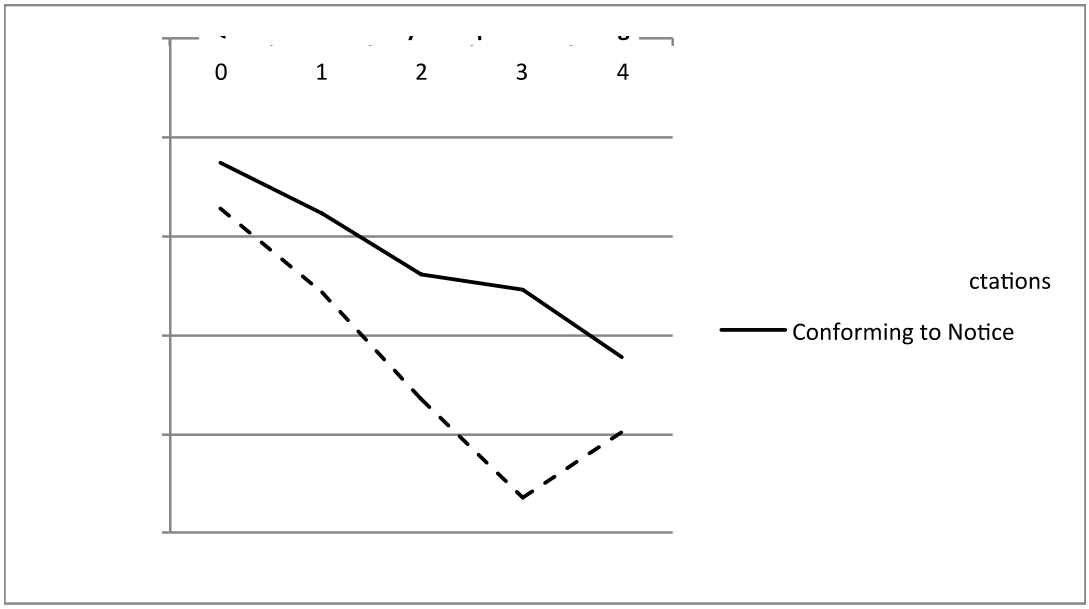


Figure 4: Privacy Notice as Tabula Rasa: Contextual factors important to meeting privacy expectations and conforming to privacy notice.

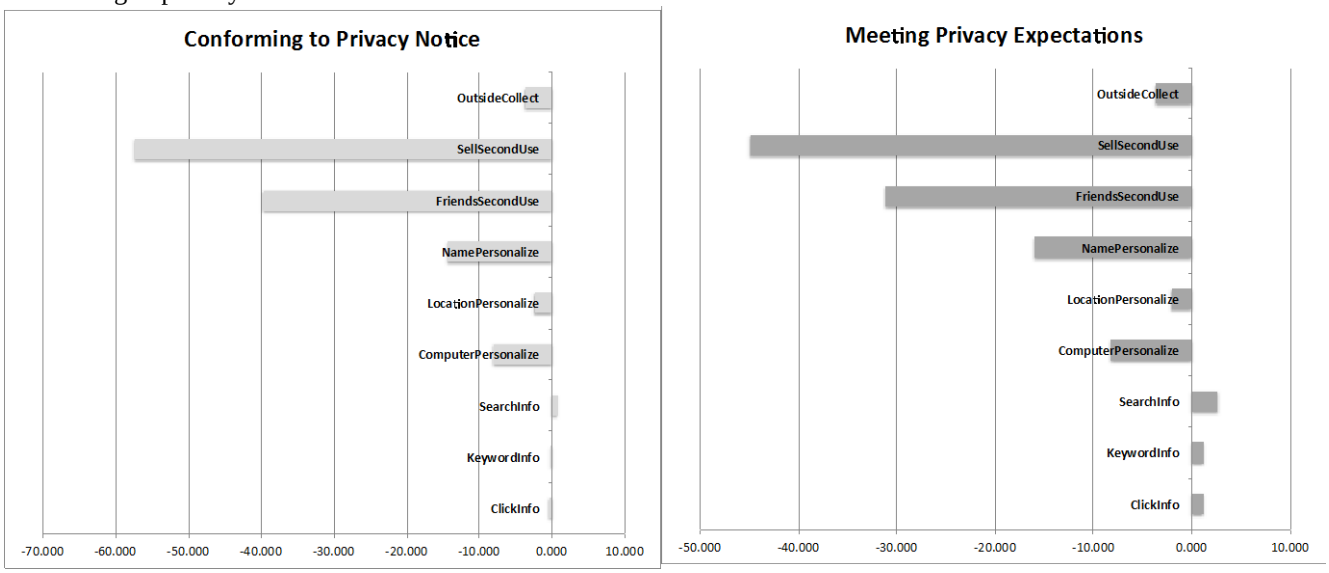
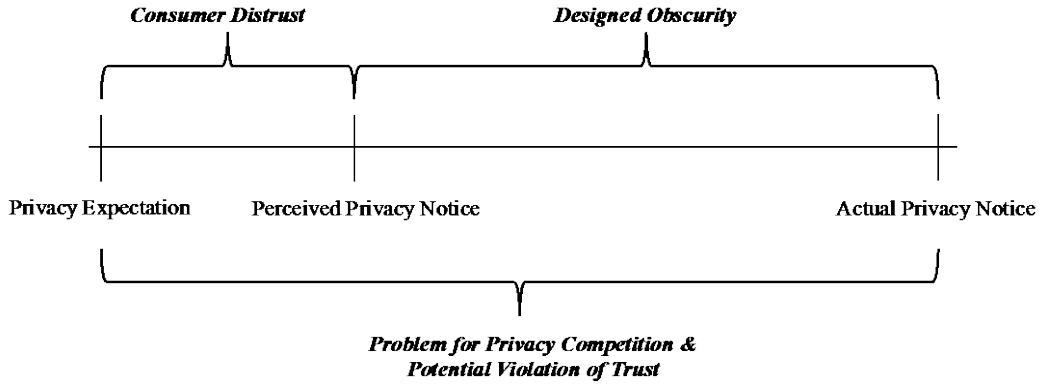


Figure 5: Perceived Privacy Notices v. Privacy Expectations



Appendix A

SAMPLE VIGNETTES:

Factors Common to All Vignettes

Factor		Dimensions		In Vignette
Context *The business of the primary organization. The underlying activity or purpose surrounding the exchange.*				CONTEXT A…CONTEXT B….CONTEXT C
		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..3…4…5…6….7 months
Frequency. *Frequency of use.*		Hours per week *(continuous)*		Very frequently…frequently…occasionally…infrequently …rarely…

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 conforms to the privacy notice.				
Strongly Disagree				Strongly Agree

Context chosen based on the following rankings:

http://www.google.com/adplanner/static/top1000/index.html# OR by country http://www.alexa.com/topsites/countries/US OR http://www.alexa.com/topsites/countries

II. 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
		3rd party tracking		an outside company's invisible tracking program …tracking company
Second 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.

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