MEASURING PRIVACY EXPECTATIONS ONLINE: A COMPARISON OF CONTEXTUAL AND INDIVIDUAL FACTORS DRIVING PRIVACY EXPECTATIONS ONLINE.

Kirsten Martin, PhD.
Kmarti33@nd.edu

ABSTRACT

A growing body of theoretical scholarship has focused on privacy as contextually defined, thereby examining privacy expectations within a specific set of relationships or situations. However, research and regulations focus on individuals' dispositions as the primary driver of differences across privacy expectations. The goal of this paper is to empirically compare the role of contextual factors versus individual dispositions in user privacy expectations. This study identifies the relative importance of contextual privacy factors driving the degree to which scenarios meet privacy expectations and examines whether and how individual characteristics impact privacy expectations. Using a factorial vignette survey, a nationally representative sample of over 1,500 respondents judged the degree to which online scenarios about targeted advertising and tracking users met privacy expectations. The results validate the use of context-based theories of privacy. However, not all factors have equal importance; the secondary use of information is the primary contextual driver of privacy expectations. In addition, the results suggest that the degree to which a scenario meets privacy expectations is dependent on both individual attributes *and* contextual factors. Privacy expectations – as the appropriate information norms within a given situation – forms the bases of privacy by design, regulations such as the FTC's commonly accepted practices, and the oft-referenced reasonable expectation of privacy in the law. The results suggest that studying and measuring privacy should involve not only an understanding of individuals' general disposition towards privacy but also the relative importance of a website's specific practices about the use of information.

Keywords: privacy online, privacy expectations, tracking, targeted advertising, factorial vignette survey.

MEASURING PRIVACY EXPECTATIONS ONLINE: A COMPARISON OF CONTEXTUAL AND INDIVIDUAL FACTORS DRIVING PRIVACY EXPECTATIONS ONLINE

1. INTRODUCTION

While most agree that privacy is important, disagreement exists on what privacy means and what it encompasses (Pavlou, 2011; Smith, Dinev, & Xu, 2011; Tsai, Egelman, Cranor, & Acquisti, 2011). Definitions of privacy vary—from private information being that which is inaccessible (Warren & Brandeis, 1890), controlled (A. F. Westin, 2003), or fairly gathered (Bennett, 1992)—and the concept remains ambiguous (Martin, 2015b; Van de Hoven, 2008). This is problematic in that researchers, regulators, and firms rely on understanding the privacy norms and expectations of users in order to create meaningful experiments, to propose commonly accepted practices for regulation (Federal Trade Commission, 2012), and to design technology, services, privacy-enhancing tools, and default settings to meet privacy expectations (Mulligan & King, 2011; Tsai et al., 2011; N. Wang, Wisniewski, Xu, & Grossklags, 2014; Xu, Crossler, & Bélanger, 2012).

A growing body of theoretical scholarship has focused on privacy as contextually defined, thereby examining privacy norms within a specific set of relationships, situations, or contexts (Anton, Earp, & Young, 2010; Belanger & Xu, 2015; Cranor, Reagle, & Ackerman, 2000; Earp & Baumer, 2003; H. Li, Sarathy, & Xu, 2010; Martin, 2015b; Nissenbaum, 2010). Context-dependent definitions of privacy view privacy expectations as the negotiated, appropriate information norms within a particular community or situation; breaking these privacy norms constitutes violating privacy (Martin, 2015b). For firms online, context-dependent approaches to privacy expectations would suggest users' definitions of privacy will depend on the type of website – medical, travel, search, etc. – as well as the specific firm policies around the tracking and use of information.

Allowing privacy norms and expectations to be dependent on context helps explain why privacy is viewed as having little shared meaning (Angst & Agarwal, 2009; Solove, 2006) and as not easily or satisfactorily defined (Smith et al., 2011). A contextual approach to privacy may also explain why research and practice struggles to identify a universally accepted, static definition of privacy. However, the focus on individuals as varying in their valuation of privacy or concern over privacy is deeply entrenched in our regulatory schemes to allow for consumer choice (Federal Trade Commission, 2010, 2012; Hoofnagle & Urban, 2014). Importantly, scholarship continually demonstrates an individual-level, general disposition towards privacy that can be a factor of prior experience, trust, or demographics as well

as a general concern or attitude towards privacy (Bansal, Zahedi, & Gefen, 2010; Hong & Thong, 2013; Smith, Milberg, & Burke, 1996a; A. Westin, 1991).

If privacy expectations vary based on a situation's contextual factors – such as who is receiving the information and how information will be used – then research, policy, and firms would focus more on identifying privacy norms and commonly accepted practices (Belanger & Xu, 2015). If privacy expectations are an individual preference (Westin, 1991), then the focus would remain on measuring individual differences as well as supporting consumer choice.

The goal of this study is to empirically compare the role of contextual factors versus individual attributes in judgments about privacy expectations online. This study allows for privacy expectations to be dependent on the context of the information exchange, identifies the relative importance of contextual factors driving privacy judgments, and examines how individual characteristics impact privacy judgments. Using a factorial vignette survey, a nationally representative sample of over 1,500 respondents judged the degree to which online scenarios about targeted advertising and tracking users met privacy expectations resulting in over 60,000 ratings. The analysis measures the relative importance of contextual factors and compares the relative strength of contextual factors versus individual dispositions in judging privacy expectations. Before explaining the methodology and study in more detail, a model of privacy judgments is first developed incorporating both individual-specific characteristics and context-dependent factors; the model is compared to two popular measurements in privacy scholarship.

This study can be seen as a first step to address the need for a more precise measurement of information privacy (Bélanger & Crossler, 2011) in identifying the relative importance of different contextual factors in driving privacy expectations online. The empirical examination of the degree to which privacy expectations are contextually versus individually defined has implications for research: understanding the drivers of privacy expectations of users online would enable practitioners to respect privacy expectations of users and support researchers in related measurements such as privacy concerns, valuations, and protection responses. In addition, privacy expectations – as the appropriate information norms within a given situation – forms the bases of privacy by design (Mulligan & King, 2011), regulations such as the FTC's commonly accepted practices (Federal Trade Commission, 2012), and the oft-referenced reasonable expectation of privacy in the law (Kugler & Strahilevitz, 2015).

2. A MODEL OF PRIVACY EXPECTATIONS

2.1 Measuring Privacy

In the quest to measure judgments about privacy, "the most challenging element of the information privacy literature is the precise measurement of the construct of information privacy" (Pavlou, 2011, p. 984). With ambiguity around privacy definitions or the operationalization of privacy (Y. Li, 2012; Pavlou, 2011; Smith et al., 2011; Tsai et al., 2011), alternative measurements are often used in privacy scholarship to explain privacy related behavior (Smith et al., 2011). Before exploring a model of judgments about privacy expectations, the related and commonly used measurements of individuals' valuation of privacy and concern for privacy are compared as in Table 1.

Table 1: Scholarship on Related Privacy Measurements

	Illustrative Research and Explanations	Strengths/Weaknesses
Valuation of Privacy	• The value of privacy is "value that individuals assign to the protection of their personal data" (Acquisti et al., 2013) which can include the amount accepted to disclose information (WTA) as well as value of protecting information (WTP) (Grossklags & Acquisti, 2007). • Context: Privacy-related behavior is dependent upon contextual factors such as cues, biases: e.g., endowment effect (Acquisti et al., 2013), framing (Grossklags & Acquisti, 2007; Tsai et al., 2011), alternatives to sharing (Ravichandran, Benisch, Kelley, & Sadeh, 2009), standards for disclosure including defaults and peers (Acquisti et al., 2012; Keith et al., 2015; Stutzman et al., 2013). • Valuation DV = Amount individual will accept to disclose information (Grossklags & Acquisti, 2007)or pay to add protections to information ((Schreiner & Hess, 2015)	• **Strengths:** Privacy is measurable and identifiable as the non-disclosure of information; users are asked to make realistic tradeoffs and reveal preferences in making decisions (Acquisti et al., 2015) • Investigates how and why users' preferences do not always translate into privacy protection actions. • **Weakness**: Individuals viewed as trading privacy when they disclose information in return for some benefits (Jiang et al., 2013; Kehr et al., 2015; H. Wang et al., 1998). The decision to disclose information can be framed as surrendering privacy (Dinev & Hart, 2006b).
Concern for Privacy	• Concern for privacy is the degree an individual expresses concern about information control or for the specific components of an instrument (Angst & Agarwal, 2009; Bansal et al., 2010; Hong & Thong, 2013; Smith et al., 1996b; Son & Kim, 2008). • Context: Concerns are also influenced by the type of information and purpose of disclosing information (Malhotra et al., 2004; Xu, Crossler, et al., 2012); e.g., "what may be a privacy concern in healthcare websites may be a very different problem for users than in social networking websites" (Xu, Teo, et al., 2012) • Concern DV = degree to which respondent expresses concern with the components of the instrument, e.g., the general collection, correction, secondary use, and security of information (Hong & Thong, 2013; Smith et al., 1996a).	• **Strengths**: Established instrument used by many in privacy scholarship; comparable across studies with high internal validity (Hong & Thong, 2013; Smith et al., 1996b)(Hong and Thong, 2013; Smith et al. 1996). Concern has been used as a *proxy* for privacy (Jiang et al., 2013; Smith et al., 2011) • **Weaknesses**: Individuals do not behave in accordance with their state 'privacy concerns' as measured by scholars (Jiang et al., 2013). • Relies upon a definition of privacy as the degree of control over information (Hong & Thong, 2013) which is not universal (Beales & Muris, 2008; Martin, 2015b). Respondent concern includes both the (in)appropriateness of the practice and the perceived risk that the practice would occur.

Judgment of Privacy Practice	• Privacy expectations, as distinct from concerns (Angst & Agarwal, 2009; Hong & Thong, 2013), are the appropriate norms of information use, gathering, disclosure within a given situation. • Context: Privacy expectations as to the appropriate information norms depends on contextual factors such as who is accessing what information and for what purpose (Martin, 2015b; Nissenbaum, 2010). • Expectation DV = degree to which scenario or practice is judged to meet or violate privacy expectations; i.e. attitude toward information practice (Schwaig et al., 2013); appropriateness of practice (Gross & Acquisti, 2005), degree individual minds the practice (Anton et al., 2010).	• **Strength:** Allows for possibility that privacy expectations vary by situation and are specific to the type of information gathered and how it is used (Nissenbaum, 2010) . • Meets the call for more precise measurement of information privacy (Bélanger & Crossler, 2011) where "the most challenging element of the information privacy literature is the precise measurement of the construct of information privacy" (Pavlou, 2011, p. 984). • **Weaknesses:** Little agreement on definitions and operationalization of definitions (Hong & Thong, 2013; Pavlou, 2011; Smith et al., 2011) requiring a more inductive study of privacy. Privacy as notoriously difficult to define (Tsai et al., 2011).

2.1.1 Valuation of privacy.

Rather than measure individuals' privacy dispositions, intentions, or judgments, behavioral privacy research examines respondents' actions such as their disclosure of information and their choice of services with different types of protections. The valuation of privacy is measured as the cost an individual is willing to pay (WTP) to uphold privacy protections or the amount respondents are willing to accept (WTA) to disclose additional information to parties (Grossklags & Acquisti, 2007; Schreiner & Hess, 2015; Tsai et al., 2011). Behavioral privacy research aims to identify users' revealed preferences by focusing on the respondents' behavior rather than only stated preferences (Acquisti, Brandimarte, & Loewenstein, 2015).

Researchers find that privacy valuations are often impacted by contextual cues and biases (Acquisti et al., 2015). Individuals are impacted by the endowment effect, where people value privacy more when they have it that when are asked to acquire protections (Acquisti, John, & Loewenstein, 2013), as well as a perceived standard of disclosure set by their peers' decisions, previously answered questions, or default settings (Acquisti, John, & Loewenstein, 2012; Stutzman, Gross, & Acquisti, 2013). The willingness to disclose can be impacted by the degree of familiarity with the recipient (John, Acquisti, & Loewenstein, 2011a) or reputation of the website (Y. Li, 2014), the application context, default setting, and type of information gathered (N. Wang et al., 2014), as well as the difference in framing between the willingness to pay (WTP) versus the willingness to accept (WTA) (Grossklags & Acquisti, 2007; Tsai et al., 2011).

The strength of this behavioral privacy research is not only capturing actual behavior rather than judgments, attitudes, or intentions, but also in measuring a single outcome so that respondents are asked to make tradeoffs between multiple factors similar to actual consumer choices outside the experiment. If disclosing information is equated to surrendering or giving up privacy (Dinev & Hart, 2006a; H. Wang, Lee, & Wang, 1998), then this research can possibly be viewed as the value people place on privacy.

However, since respondents regularly disclose information while retaining expectations of privacy, the majority of behavioral privacy research frames the findings as the willingness to provide personal information given the perceived costs, protections, and benefits (Hann, Hui, Lee, & Png, 2008; Xu, Zhang, Shi, & Song, 2009).

2.1.2 Concern for privacy

Privacy research has also focused on measuring the privacy concerns of consumers as the degree to which respondents express concern about information being fairly gathered, accessed, controlled, or used (Angst & Agarwal, 2009; Dinev & Hart, 2006b, p. 2; Hong & Thong, 2013; Smith, Milberg, & Burke, 1996b; Son & Kim, 2008; Xu, Luo, Carroll, & Rossen, 2011). The subject of privacy concerns may be broad, such as "How concerned are you about threats to your privacy…" (Nguyen, Bedford, Bretana, & Hayes, 2011), or more specific, such as with the concern for information privacy score (Smith et al., 1996b), or Internet privacy concerns (Hong & Thong, 2013). Privacy concerns have been used to explain consumers' willingness to render personal information (Dinev & Hart, 2006a) and transaction activity (Pavlou, Liang, & Xue, 2007).

Importantly, privacy concerns are individual-level measurements of the degree to which a respondent is concerned about their general ability to control information. Yet, individuals do not behave in accordance with their privacy concerns as measured by scholars (Jiang, Heng, & Choi, 2013). One possible issue is the translation from a general 'concern' as an individual disposition to the perception of a particular context in practice (H. Li, Sarathy, & Xu, 2011; Xu, Wang, & Grossklags, 2012). A second important challenge facing scholars is the lack of a well-understood, consistent definition of privacy across individuals and contexts. Privacy concern scales rely heavily on a *control* definition of privacy where privacy is the ability of the individual to control who, how and to what extent information is communicated to others (Hong & Thong, 2013; A. F. Westin, 2003); yet control definitions of privacy are only one possibility which come under scrutiny since individuals hold privacy expectations regardless of their degree of control over their information (Beales & Muris, 2008; Martin, 2015b). In the absence of a settled definition of privacy, privacy concern has been used as a proxy for privacy in scholarship (Smith et al., 2011), leaving open the possibility for a different measure of privacy and privacy expectations in scholarship (Pavlou, 2011).

2.1.3 Privacy expectations

Less work has been done to identify respondents' specific privacy expectations as a distinct construct (Angst & Agarwal, 2009; Bélanger & Crossler, 2011; Jiang et al., 2013). Privacy expectations are the context-appropriate information norms around what information is gathered and how information is used by a firm; breaking these privacy norms constitutes violating privacy (Martin, 2015b).[1]

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 or used. Such privacy expectations are formed within a social contract where communities develop rules about disclosure and dissemination of information. Similar measures of users' normative judgment of the appropriate use and collection of information include respondents' comfort level with a practice (Lin et al., 2012), the respondents' perceived intrusiveness of a practice (Zhang, Shih, & Weitzner, 2013), whether the respondents mind the practice (Anton et al., 2010), and whether the practice is perceived as appropriate (Acquisti & Gross, 2006). Such examinations allow individuals to normatively judge the specific types of practices of the firm as respecting or violating privacy norms and expectations.

Privacy expectations are examined in marketing (Milne & Bahl, 2010; Phelps, Nowak, & Ferrell, 2000) and information systems (Spiekermann & Cranor, 2009). As noted by Gross and Acquisti (2005) "privacy expectations may not be matched with privacy reality." However, when firms' privacy practices *do* match the privacy norms and expectations, users are more willing to disclose information (Xu, Wang, et al., 2012) and pay a premium (Schreiner & Hess, 2015; Tsai et al., 2011).

Two related theories examine privacy expectations within a specific set of relationships or contexts and have identified and support a theoretical, systematic framework for defining privacy expectations with relevant categories of factors. Both privacy as contextual integrity (Nissenbaum, 2010, 2011) and privacy as a social contract (Martin, 2015b) view privacy expectations as the developed rules about what information is gathered by whom and for what purpose within a particular community or relationship.

For Nissenbaum, "the crucial issue is not whether the information is private or public, gathered from private or public settings, but whether the action breaches" the contextually understood information norms (Nissenbaum, 2004, p. 134). More specifically, the very function of privacy expectations is

[1] Privacy concerns differ from privacy expectations (Angst & Agarwal, 2009; Hong & Thong, 2013) and that is no exception here. First, where concerns focus on the individual's assessment, privacy expectations are defined by the situation, relationship, or context. In addition, privacy concerns incorporates the degree to which the practice is appropriate as well as the risk belief or probability or risk that the practice will occur (Dinev & Hart, 2006a) to identify areas of focus for firms or regulators to decrease users' concerns. For example, low concern items would include the U.S. government putting cameras inside homes (low probability and not appropriate) as well as Google maps collecting location data (high probability and appropriate).

developed within a situation. The rules around what information can be disclosed and gathered and for what purpose develops within a particular community or context. In other words, "individuals have highly particularized judgments about the appropriateness of what, why, how, and to whom information flows" (Martin, 2012a).

2.2 Framework and Model of Privacy Judgments.

While acknowledging the difficulty of identifying a well-accepted definition, several factors have been found to influence the *meaning* of information privacy (Pavlou, 2011; Smith et al., 2011). For privacy as contextual integrity (Nissenbaum, 2010) or for privacy as social contract (Culnan & Bies, 2003; H. Li et al., 2010; Martin, 2012a; Xu et al., 2009), privacy expectations are the norms or rules about information flow in a particular situation which takes into account factors such as the type of information, how information is used, and who has access to information. This framework is also based on previous empirical studies on how factors in a situation impact normative judgments about privacy as outlined below. The factors work in combination: privacy expectations are around who can receive specific information and what uses are appropriate within a particular context or community.

- ***Context.*** For some, context is broad such as the technology (Martin, 2012b; Xu, Teo, Tan, & Agarwal, 2012) or location (Toch et al., 2010). Here privacy expectations are dependent on the context or community defined as the structured social setting with specific roles, relationships, power structures, norms, and internal values (Martin, 2015b; Nissenbaum, 2010). For example, the privacy expectation have been found to depend on the type of website such as retail, medical, or financial (Earp & Baumer, 2003) or the difference between banking, news, weather, sports contexts (Cranor et al., 2000).
- ***Recipient.*** Information is disclosed with a specific set of appropriate recipients (Anton et al., 2010; Nissenbaum, 2010), and researchers regularly find disclosure to particular third parties to be a violation of privacy (Cranor et al., 2000).
- ***Information.*** The type of information gathered impacts users' comfort in sharing (Cranor et al., 2000), what users mind (Anton et al., 2010), and users' willingness to provide information (Earp & Baumer, 2003). Information seen to be a violation of privacy expectations are referred to as sensitive (Malhotra, Kim, & Agarwal, 2004) (John, Acquisti, & Loewenstein, 2011b) or personal: e.g., the differences between food preferences and information about sexual preferences as impacting users' normative judgment (Acquisti & Gross, 2006; Norberg, Horne, & Horne, 2007).
- ***Use.*** How information is used within a context impacts meeting privacy expectations (Nissenbaum, 2010) such as using information for marketing versus customizing the experience (Anton et al., 2010)

or as found when the use of information impacts users' comfort in sharing information (Cranor et al., 2000).

Based on these factors, a judgment about meeting privacy expectations would be defined as a function of the context *j*:

$$Y_j = \text{Privacy Judgment}_j = g(\text{information}_j, \text{use}_j, \text{recipient}_j) \quad (1)$$

A second stream of privacy scholarship seeks to identify individual-specific dispositions towards privacy. Individual differences such as self-esteem, alienation, computer anxiety, and general concern for privacy impact attitudes towards information practices (Schwaig, Segars, Grover, & Fiedler, 2013). Similarly, privacy pragmatists (Harris Interactive, 2003; A. Westin, 2001) are defined as those individuals willing to permit the use of their information (a) if they are given a rationale and tangible benefits and (b) if they sense that safeguards are in place to prevent misuse (Beales & Muris, 2008, p. 118 fn 29). Importantly, scholarship continually demonstrates an individual-level, general disposition towards privacy that can be a factor of prior experience, trust, or demographics as well as a general concern or attitude towards privacy.

The approaches above can be framed in tension: privacy expectations are either contextually defined or are dependent on an individual-specific attitude toward privacy. However, privacy expectations may be a product of both the context of the exchange and the individual's disposition towards privacy. For example, context can be seen as overwhelming individual disposition (H. Li et al., 2011); and an individual's concern for privacy may be influenced by context (Malhotra et al., 2004). Privacy expectations can be measured as a general attribute of the individual as well as specific to a context (Angst & Agarwal, 2009; H. Li et al., 2010; Xu, Wang, et al., 2012), where a judgment about meeting privacy expectations would be dependent upon the contextually defined privacy expectations as well as the individual's attitude or disposition about privacy:

Y_{ij} = Privacy Judgment of individual *i* about scenario *j*.

$$Y_{ij} = f(\text{Individual}_i) + g(\text{Context}_j) \quad (2)$$

Combining equation (2) with Equation (1) results in (3).

$$Y_{ij} = f(\text{Individual}_i) + g(\text{information}_j, \text{use}_j, \text{recipient}_j) \quad (3)$$

To capture such highly particular and situation based privacy expectation can be difficult in empirical research. Research must provide realistic, highly particular situations (Cranor et al., 2000). In order to test "the relationship between various firm-level practices and their affects on consumers' privacy perceptions" (Lanier & Saini, 2008), detailed scenarios are necessary considering many users are unaware of firm practices around the gathering, use, and disclosure of user information. Such an approach meets the call for more research to "consider salient beliefs and contextual differences at a specific level" (Malhotra et al., 2004, p. 349). The method chosen to capture such detail is explored below.

3. METHODS

The goal of this research is to empirically examine the factors driving individuals' judgments about privacy expectations online and to compare how contextual factors impact meeting privacy expectations relative to individual attributes. The factorial vignette survey methodology was utilized to capture the highly particular contextual factors that may (or may not) drive privacy expectations, and traditional survey methodology captured individual attributes.

Developed to investigate human judgments (Jasso, 2006; Rossi & Nock, 1982; Wallander, 2009), a factorial vignette survey has the respondent evaluate a series of vignettes describing a hypothetical unit of analysis (here, a website). The vignette factors describing the scenario are the independent variables; each factor has multiple levels which are systematically varied. These factors and their associated coefficients are referred to as the '*equations-inside-the-head'* (Jasso, 2006) of respondents.

The factorial vignette survey methodology (FVSM) offers a unique approach to systematically change multiple contextual factors simultaneously in order to create more realistic scenarios while utilizing a simple judgment for the rating task: the degree to which the scenario meets privacy expectations. The factorial vignette survey methodology best simulates the contextual factors for the empirical examination of the context-dependent model developed above while allowing the normative judgments to be inductively examined.

The FVSM was created to capture multifaceted judgments indirectly by presenting respondents with stimuli that resembles real-world evaluations and force them to make trade-offs between several dimensions (Auspurg, Hinz, Liebig, & Sauer, 2014). As such, the FVSM was designed to avoid social desirability bias by indirectly measuring the factors that drive normative judgments rather than asking the respondents directly. Normative judgments, such as privacy expectations, are notoriously difficult to examine as respondents may attempt to bias answers in an attempt to appear more ethical, and respondents may have difficulty identifying and articulating the reasoning behind their judgments. Finally, the analysis permits the identification of both socially shared privacy judgments as well as differences across subgroups (Auspurg et al., 2014) which is theoretically suggested above and forms the basis of the research question.

3.1 Study Design.

The vignettes for this study were constructed by varying several online privacy factors for both tracking users as well as targeted advertising online based on the theoretical framework above. When designing a factorial vignette survey, respondent fatigue is addressed by considering the number of factors in each

vignette, the number of levels for each factor, as well as to the number of vignettes rated by each respondent. In order to simplify the vignettes, the factors driving privacy expectations online were split between tracking users and targeted advertising thereby minimizing the cognitive load on users. This tactic lowered the number of factors in *each* survey but then required two samples to be gathered rather than one. The number of levels for each factor was limited and continuous variables were also used when possible to decrease the cognitive load on respondents.

In addition, the number of vignettes per respondent is a balance between the statistical needs and the amount of time required for a single respondent to take the survey. As noted by (2006), the number of vignettes must be "large enough to enable precise estimation of respondent-specific equation yet small enough to prevent respondent fatigue." Previous factorial vignette survey research has been limited by the mode of administration as researchers relied upon face-to-face administration of paper or oral vignettes; many factorial vignette surveys employed 60-80 vignettes per respondent (Jasso, 2006). Here, the use of computer programming to design and create the vignettes and web-based tools to administer the survey alleviated many of the logistical limitations on the number of factors and levels to include. A deck of 40 vignettes for each respondent was randomly created with replacement as the respondent was taking the survey. Using random samples ensures orthogonal vignette factors (Ganong & Coleman, 2006).

For each rated vignette, the associated rating, factor levels, and the vignette script was preserved as well as the vignette sequence number. Each respondent was assigned one type of vignette – either targeted advertising or tracking users online.

3.2 Operationalization

3.2.1 Contextual Vignette Factors

The vignettes contained scenarios of tracking users and targeted advertising online based on the model of privacy judgments developed above in Equation 3. Contextual factors such as the overall purpose of the website (context) and the type of information gathered were included across both surveys. Each is described below and the sample is in Table 2:

Context: The website context – e.g., playing games, planning travel, participating in social networking, navigating using maps, watching videos, banking, shopping. In order to systematically vary the online contexts of the vignettes, three publically available rankings of website activity were used to compile a list of ten distinct contexts online: movies, social networking, medical, retail, search, news, video sharing, travel, banking, and payment service.

Information: Four types of information were systematically varied in the vignettes for both the targeted advertising and tracking users vignettes: where users click on the page, the search terms

entered, keywords on the page, and general demographic information. In addition, vignettes included additional personalized information, such as names, references to friends, or location, not disclosed by the individual.

Recipient: The data collection actor was the organization collecting information and varied such as the website or 3rd party advertiser, primary website, or data aggregator. For targeting vignettes, the advertisement could be from the primary website or a third party site.

Use/Secondary Use: How the data was reused or stored varied for vignettes. For tracked information, data can be stored for a particular length of time, used for future targeted ads, used for ads targeting friends, or sold to a data broker/aggregator. For targeting vignettes, the use of the data was for advertising.

Table 2: Sample Vignettes for Targeted Advertising and Tracking Users Surveys

SAMPLE VIGNETTES:
Targeting Sample Vignette: You are working on an online banking website that you have used frequently for five months. The online banking site places an advertisement for a new website's products based on search terms you typed. In addition to your activities on the online banking site, the advertisement also uses your location to tailor the ad.
Tracking Sample Vignette: You are shopping on a retail website that you have used rarely for 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.
Rating Task: This website meets my privacy expectations (strongly agree….strongly disagree)

3.2.2 Dependent Variable

For each vignette, respondents were asked to judge the degree to which the situation in the vignette met their privacy expectations. Respondents were given a rating task: 'Tell us how much you agree with the statement below. Using a sliding scale from -100 to 100, with -100 indicating 'strongly disagree' and 100 indicating 'strongly agree'. The respondents were given the prompt, 'This website meets my privacy expectations.'

The rating task captures the complicated normative judgment of the respondent of the realistic scenario in the vignette. The rating task should be as open as possible to "faithfully represent the possible variable continuum in the respondent's head and that allows the rater maximum freedom in estimating magnitudes" (Jasso, 2006, p. 344). The use of a slider with only the end-points specified accomplished this goal by not locking the respondent into specific buckets as when using a 7 option task and giving the respondent maximum freedom in differentiating judgments.[2]

[2] Measuring privacy expectations here differs slightly from measuring consumer expectations or customer satisfaction in the marketing literature (Zeithaml, Berry, & Parasuraman, 1993a). Importantly, ambiguity about

3.2.3 Individual-Specific Factors

In addition to the demographic information in Table 3, experience online has been found to be an important factor in attitudes and judgments about information management and privacy. The panel data, therefore, includes whether or not the respondent previously had Internet access prior to being included in the KnowledgeNetworks panel. Internet experience (how long someone has been an Internet user) has been correlated with their awareness of and engagement in a wider range of online activities (Madden & Rainie, 2002). This has also been found more recently in regards to broadband (Horrigan, 2013). Prior experience to a service impacts consumer expectation of both what is possible and what is ideal in a given situation (Boulding, Kalra, Staelin, & ZElTHAML, 1993): expectations depend on knowledge of what is possible as well as what is actually occurring (Zeithaml, Berry, & Parasuraman, 1993b).

In addition, two individual beliefs or attitudes were captured to test the influence of individual-specific factors in making privacy judgments as in Equation (3). First, trust has been found to be closely related to privacy (Keith, Babb, Lowry, Furner, & Abdullat, 2015; Pavlou, 2011, p. 983), where trust, as a predictor of behavior, may be more important than privacy concerns (Eastlick, Lotz, & Warrington, 2006; Sultan & Rohm, 2004; Van Slyke, Shim, Johnson, & Jiang, 2006). Following the call for privacy scholarship to include the effect of trust (Pavlou et al., 2007; Van Slyke et al., 2006), a rating captured respondents' general trust in websites as an institution (Gefen & Pavlou, 2012; Kehr, Kowatsch, Wentzel, & Fleisch, 2015). 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 (Dinev & Hart, 2006a; Smith et al., 1996b; Xu, Wang, et al., 2012). Accordingly, the second rating task stated, 'In general, I believe privacy is important.'

3.3 Subjects

The surveys were first given to 10-12 researchers and practitioners to check for realism, readability, and comprehension. In addition, the surveys were piloted on Amazon Mechanical Turk (MTurk) as well as

consumer expectations in marketing is around the prompt "What do you expect from [FIRM]?" and is open-ended. Here, the ambiguity could be around whether the expectations are ideal or merely adequate. Adequate privacy expectations could fall victim to the resignation found in privacy surveys – users become resigned to bad behavior. This interpretation would suggest the results may be conservative and respondents have stricter privacy expectations than measured here.

with students at a private, mid-Atlantic university. A comparison of the theoretical generalization possible across pilot and live samples is in the Appendix.[3]

The sample for the studies recruited by GfK/KnowledgeNetworks, which is an online research panel representative of the entire U.S. population. GfK/KnowledgeNetworks panel members are randomly recruited through probability-based sampling. Households are provided with access to the Internet and hardware if needed. For an overview of the GfK/KnowledgeNetworks sampling methodology and a comparison to the pilot tests on Turk, please see Appendix A.

For the two surveys, 1,520 respondents rated 40 vignettes resulting in 62,960 rated vignettes or observations (targeting: 754 respondents and 31,160 vignettes; tracking: 766/31,800). Summary statistics on the samples for both targeted advertising and tracking users are in Table 3.

Table 3: Sample Demographics for Targeted Advertising and Tracking Users Surveys

	Targeted Ad Survey	Tracking Users Survey		Targeted Ad Survey	Tracking Users Survey
Age – 7 Categories	Percent	Percent	**Race / Ethnicity**	Percent	Percent
18-24	10.0	10.1	White, Non-Hispanic	73.3	73.5
25-34	16.3	15.0	Black, Non-Hispanic	9.6	9.1
35-44	17.2	18.8	Other, Non-Hispanic	3.1	3.0
45-54	16.6	20.0	Hispanic	10.0	10.3
55-64	21.2	17.6	2+ Races, Non-Hispanic	4.1	4.1
65-74	13.5	13.7			
75+	5.2	4.8			
Education (Categorical)	Percent	Percent	**HH Internet**		
Less than high school	8.0	9.9	**Access (PPNET)**	Percent	Percent
High school	30.5	27.4	No	19.5	19.5
Some college	29.2	28.5	Yes	80.5	80.6
Bachelor's or higher	32.4	34.2			

3.4 Quality Check

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. Respondent fatigue was checked in two ways. First, regression analysis was run on subsamples of the total pool: the first and

[3] MTurk proved to be a strong substitute for the nationally-represented sample described below; whereas the student sample was significantly different. Additional research implications are discussed in the discussion and explored in Appendix A.

last 20 vignettes rated and after dropping the first and last 5 vignettes rated for each respondent. The results show that the rating task averages – the overall average rating that the vignettes meet privacy expectations – decreases slightly over the course of the vignettes. However, the relative importance of different vignette factors did not change nor did the standard deviation of the dependent variable.

Second, a variable was added for first 5 and last 5 (First5Qs and Last5Qs) for both surveys and the significance was tested in the multi-level regression analysis. Using the analysis of the dummy variables, the first 5 vignettes were rated higher on average for targeting vignettes (coefficient of "First5Qs" in regression of rating task on all factors is +4.56, $p < 0.01$) and tracking vignettes (+5.03, $p < 0.01$). The last 5 vignettes also received a lower rating task on average for tracking vignettes only (Last5Qs = -1.96, $p < 0.01$) but are rated statistically on average the same for targeting vignettes (Last5Qs = -0.37, $p = 0.50$). The rating for the first 5 vignettes differed more than the ratings of the last 5 vignettes – when both are taken into account simultaneously. This would suggest that the first 5 ratings were *more* of an outlier than the last five ratings. This finding is consistent with previous analysis of factorial vignette surveys with the respondents' *learning curve* – presumably from the novelty of the survey design (Martin, 2012a).

4. RESULTS

The goal of this study is to empirically examine the factors driving individuals' judgments about privacy expectations online and to compare how general contextual factors impact meeting privacy expectations relative to individual variables. Table 4 contains the survey data for both the targeted advertising and tracking users surveys. Overall, scenarios around targeted advertising met expectations of privacy to a greater extent (mean = -29.83) compared to scenarios about tracking users online (mean = -47.00). Both types of vignettes, on average, did not meet privacy expectations of respondents.

TABLE 4: Targeting and Tracking Vignette Survey Samples.

	Targeted Adv. Vignettes		Tracking Users Vignettes	
Respondents	754		766	
Vignettes	30,160		30,640	
	Mean	Std. Dev.	Mean	Std. Dev.
Age	48.00	16.91	47.70	16.61
Male	50.3%		51.7%	
Privacy is Important	71.54	38.90	71.52	41.50
I trust websites	-6.40	42.42	-3.56	44.41
Mean (DV)	-29.83	40.31	-47.00	38.66
sd (DV)	30.23	17.82	30.22	18.73
_eq2_R2	0.67	0.19	0.68	0.16

The analysis below focuses first on the importance of contextual factors and individual attributes on privacy expectations separately. The analysis then turns to compare the importance of individual attributes versus contextual factors in driving privacy expectations.

4.1 Contextual Factors.

In order to identify the relative importance of each contextual factor in judgments about meeting privacy expectations, each block of vignette factors – context, information, recipient, secondary use, etc. – was included in a hierarchical model and the results of the regressions are in Tables 5a and 5b. Multi-level regression was used and the explained variance and intraclass correlation coefficient (ICC) for each equation is included.

Generally, the factor capturing how the information was used after disclosure was more important in meeting privacy expectations than the type of information collected. For example, the secondary use of data, such as selling information to a third party ($\beta = -21.00$, $p < 0.01$) or using the information to target friends ($\beta = -17.28$, $p < 0.01$), significantly impacts meeting privacy expectations in Table 5a in comparison to using collected information for an advertisement. In addition, for targeted ads, personalized additional information, such as the use of friends ($\beta = -13.58$) or the individual's name ($\beta = -13.25$), had a greater impact on the degree to which vignettes met privacy expectations in comparison to the general type of information (e.g., collecting demographic, search, or click information).

Tables 5a and 5b are also important to illustrate what is *not* significant in meeting privacy expectations. The general type of information initially disclosed does not help explain judgments about meeting privacy expectations for targeted advertising and tracking users online. As a block of factors, the type of information was not significant for targeted advertising ($\chi^2 = 3.71$, Δ d.f. = 3, $p = 0.29$) and tracking users ($\chi^2 = 1.95$, Δ d.f. = 3, $p = 0.58$) meaning the model is not improved when the type of information gathered (click, keyword, search, demographic) is included.

The results suggest that not all contextual factors have equal weight in meeting or violating privacy expectations. In regards to websites contexts, banking, payment services, and medical websites differed significantly from retail websites (the null) for both targeted advertising and tracking users online. However, the secondary use of information and personalized information dominates the contextual drivers of privacy in Tables 5a and 5b, thus suggesting that the type of information matters significantly less than the privacy practices of the website after the information is gathered.

Table 5a: Targeting Vignette Hierarchical Model Regressions**

Fixed Effects Added:	Model 1a n/a	Model 1b + contexts	Model 1c information	Model 1d addl info	Model 1e recipient	Model 1f Indiv control
Context (null = Retail)						
BankingCxt		**-8.09**	**-8.10**	**-8.03**	**-8.03**	**-8.03**
VideoCxt						
TravelCxt						
MedicalCxt		**-3.58**	**-3.58**	**-3.53**	**-3.53**	**-3.54**
MovieCxt						
NewsCxt						
PaymentCxt		**-10.12**	**-10.13**	**-10.23**	**-10.25**	**-10.26**
SearchCxt						
SocialCxt					*-1.73*	*-1.74*
Information (null = Demo)						
ClickInfo						
KeywordInfo						
SearchInfo						
Additional Info (null = Null)						
FriendsEnhance				**-13.58**	**-13.57**	**-13.58**
LocationEnhance				**5.88**	**5.87**	**5.88**
NameEnhance				**-13.23**	**-13.24**	**-13.25**
Recipient (null = retarget)						
FamiliarAd						
PrimaryAd					**1.59**	**1.59**
Control Variables						
Male						*5.03*
Age						**-0.73**
TrustSites						**0.25**
PrivacyImportant						**-0.22**
_cons	-29.83	**-25.79**	**-26.44**	**-21.06**	**-21.36**	**23.60**
Model Statistics						
N	30,160					
ICC	56.40%	56.73%	56.73%	58.25%	58.27%	51.94%
sd(_cons)	39.90	39.92	39.92	39.95	39.95	35.15
R2 (explained variance)		0.43%	0.00%	2.47%	0.03%	22.60%
Deviance	303,184	302,813	302,809	301,027	301,002	300,812
df	3	14	17	20	22	27
log ratio X2	n/a	310.57	3.69	1782.63	24.71	189
p	n/a	0.00	0.30	0.00	0.00	0.00

**Notes for Tables 5a and 5b:

1. *Due to space constraints, coefficients bolded for p <= 0.01; grey for p <= 0.05; blank for p > 0.05.*
2. *ICC = Intraclass Correlation Coefficient = % of variation attributable to the group variable (individual)*
3. *sd(_cons) = the st dev of the mean (_cons) for that equation across individuals. Larger standard deviation of the intercept suggests the equation may shift based on the individual.*

Explained Variance = how much do the incremental variates help explain the DV

Table 5b: Tracking Vignette Hierarchical Model Regressions

Fixed Effects Added:	**Model 1a** n/a	**Model 1b** contexts	**Model 1c** info	**Model 1d** addl info	**Model 1e** second use	**Model 1f** recipient	**Model 1g** indiv control
Context (null = Retail)							
BankingCxt		**-11.20**	**-11.21**	**-11.24**	**-11.09**	**-11.12**	**-11.11**
VideoCxt		**-1.99**	**-2.00**	**-2.06**	-1.58	-1.62	-1.62
TravelCxt							
MedicalCxt		**-2.75**	**-2.76**	**-2.68**	**-2.44**	**-2.51**	**-2.49**
MovieCxt							
NewsCxt							
PaymentCxt		**-9.81**	**-9.81**	**-9.82**	**-9.29**	**-9.32**	**-9.32**
SearchCxt							
SocialCxt							
Information (null = Demo)							
ClickInfo							
KeywordInfo							
SearchInfo							
Addl Info (null = Null)							
ComputerPersonalize				**-2.85**	**-2.90**	**-2.91**	**-2.90**
LocationPersonalize				1.07	**1.15**	**1.12**	**1.14**
NamePersonalize				**-6.28**	**-6.08**	**-6.06**	**-6.06**
Second Use (null = Retarget)							
FriendsSecondUse					**-17.28**	**-17.28**	**-17.28**
SellSecondUse					**-20.99**	**-21.00**	**-21.00**
Recipient (null = Primary)							
OutsideCollect						**-2.21**	**-2.20**
Storage							
StorageMths						**-0.34**	**-0.34**
Control Variables							
Male							
Age							**-0.40**
TrustSites							**0.24**
PrivacyImportant							-0.28
_cons	**-47.00**	**-44.58**	**-44.87**	**-43.22**	**-30.79**	**-28.32**	**14.25**
Model Statistics							
N	30,640						
ICC	53.62%	53.99%	54.00%	54.11%	55.80%	55.84%	49.93%
sd(_cons)	38.23	38.26	38.26	38.24	38.21	38.21	33.94
R2 (explained variance)	n/a	0.49%	0.00%	0.33%	3.19%	0.06%	21.12%
Deviance	308,733	308,348	308,346	308,174	306,082	306,039	305,861
df	3	14	17	20	22	24	29
log ratio X2	n/a	382.48	2.06	172.09	2092.09	43.41	177.79
p	n/a	0.00	0.56	0.00	0.00	0.00	0.00

4.2 Individual Factors.

In order to examine the role of individual factors in privacy expectations, the vignette rating task was regressed on both the individual factors as well as contextual factors in Tables 5a and 5b.

Age significantly impacts the degree to which vignettes meet privacy expectations for both targeting ($\beta = -0.73$, $p < 0.01$) and tracking ($\beta = -0.40$, $p < 0.01$) vignettes. In other words, for both targeting and tracking online, older respondents have their privacy expectations met less for the same set of scenarios. However, age does not impact the generic concern about privacy rating ("Privacy is important.

The general 'privacy is important' rating was significant to meeting privacy expectations of both targeting ($\beta = -0.22$, $p < 0.01$) and tracking ($\beta = -0.28$, $p = 0.07$) vignettes. In other words, for every additional +1.0 the respondent stated they agreed that privacy is important (on a scale of -100 to +100), the specific vignettes were rated to meet privacy expectations -0.22 less for targeting vignettes and -0.28 less for tracking vignettes. In addition, the general trust in the institution of websites significantly impacted meeting privacy expectations for both targeting ($\beta = 0.25$, $p < 0.01$) and tracking ($\beta = 0.24$, $p < 0.01$) vignettes.

4.3 Role of Individual versus Contextual Factors.

The relative contribution of contextual factors versus individual attributes is examined using two measures. First, the intraclass correlation coefficient (ICC) produced in multi-level regressions measures the percent of variation in the dependent variable (meeting privacy expectations) that is attributable to individuals (the grouping variable). Even when including all contextual and control variables as in Models 1f and 1g (Tables 5a and 5b respectively), 51.9% of the variance in privacy judgments remains attributable to the individual for targeting vignettes and 49.9% for tracking vignettes. A significant portion of the judgment that the scenario meets privacy expectations is explained by differences across individuals and not within contextual factors.

Second, when each block of factors is added to the hierarchical modeling in Tables 5a and 5b, the explained variance measures how much the incremental variables explain the dependent variable's variance (meeting privacy expectations) compared to the variance of the outcome in the previous model. The largest explained variance of the contextual factors is the secondary use of information (2.5%) and the use of personalized data enhancement (3.2%) for tracking vignettes. In comparison, the control variables explain 22.6% of the variance for targeting vignettes and 21.1% for tracking vignettes.

These results suggest that both individual factors and contextual information practices impact meeting consumers' privacy expectations online. Yet, the variance in rating vignettes as meeting privacy expectations that is attributable to individuals remains high, meaning individuals vary in the relative importance of the contextual factors driving privacy expectations online. While privacy expectations may vary based on contexts online, more work needs to be done to understand the variance still attributable to individuals.

4.4 Post Hoc Analysis: Impact of Individual Factors on the Importance of Contextual Factors

The model first tested in Tables 5a and 5b assumes that individuals may vary in their privacy expectations through a random intercept model: the intercepts may vary across individuals but coefficients of the contextual factors are assumed to be common (also called a random intercept with fixed effects model). Models 1a-1g in Tables 5a and 5b are the random intercept with fixed effects models as the contextual factors (i.e. the fixed effects) are added one block at a time.

However, given the size of the variance across individuals in Tables 5a and 5b, individuals may have different privacy equations within a particular context, where the relative importance of factors varies across individuals. For example, some individuals may be particularly sensitive to a scenario being in the banking context where others might vary in their assessments around social networking websites. A random slope model measures variance of the *slopes* or the coefficients of the contextual factors across individuals (Chung et al. 2013). In fact, four website contexts vary significantly across respondents for both tracking users and targeted advertising: banking, payment services, medical, and social networking.

To further explain how Internet experience impacts privacy expectations and the relative importance of contextual factors, the subsample of those with and without Internet access is described in Table 6. The results suggest that respondents with Internet experience self describe as finding privacy more important and trust websites to a greater extent. In addition, for both surveys, respondents with greater online experience have greater certainty in their privacy judgments: the respondent-level equation has a calculated respondent-R^2 to capture the certainty of the respondent in rating the vignettes. The respondent R^2 is greater for both targeting ($R^2 = 0.68$) and tracking vignettes ($R^2 = 0.68$) as compared to respondents without Internet access ($R^2 = 0.64$ and 0.65 respectively).

Table 6: Comparison of control variables for respondents with and without prior Internet access.

Targeting Vignettes	PPNET Previous Internet Access			
	Y	N	t-value	p
Privacy-is-Important	73.80	62.19	-3.27	0.00
Trust Sites	-4.45	-14.46	-2.58	0.01
R^2	0.68	0.64	-2.63	0.01
DVMean	-30.17	-28.42	0.47	0.64
Tracking Vignettes	PPNET			
	Y	N	t-value	p
Privacy-is-Important	73.52	63.22	-3.27	0.000
Trust Sites	-0.45	-16.43	-2.58	0.000
R^2	0.68	0.65	-2.63	0.000
DVMean	-48.79	-39.60	0.47	0.000

Finally, the samples were split into those with and without Internet access, and the rating task was regressed onto the vignette factors for each subsample. The results are shown in Figure 1 and 2. Those with and without prior Internet access, as the proxy for Internet experience, rate the targeted advertising vignettes statistically the same yet take into consideration different contextual factors. Figure 1 and 2 illustrate how respondents with previous Internet access take into consideration more contextual factors in rating the vignettes to meet their privacy expectations and rely *less* on the individual attributes. A respondent's institutional trust in websites, for example, is less important for those with Internet access (TrustSites = 0.24, $p < 0.01$) compared to those without internet access (TrustSites = 0.35, $p < 0.01$) in meeting privacy expectations.

Figure 1: Relative Importance of Contextual Factors By Respondent Experience Online – Targeted Ad Vignettes

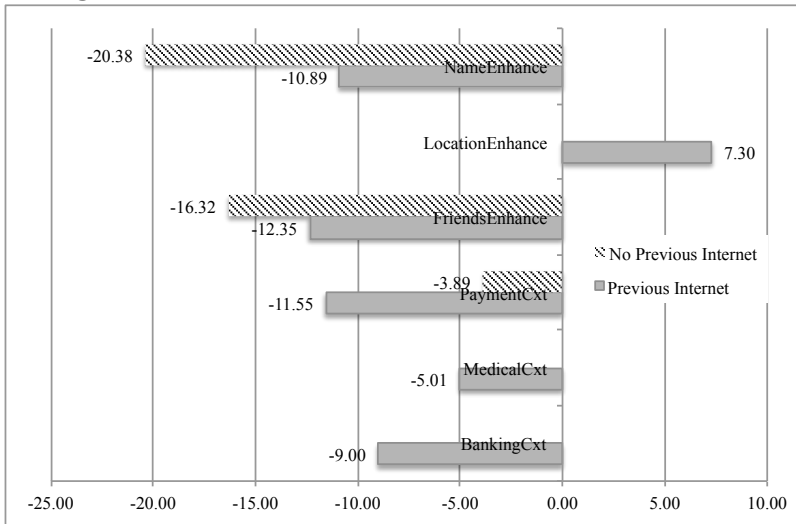
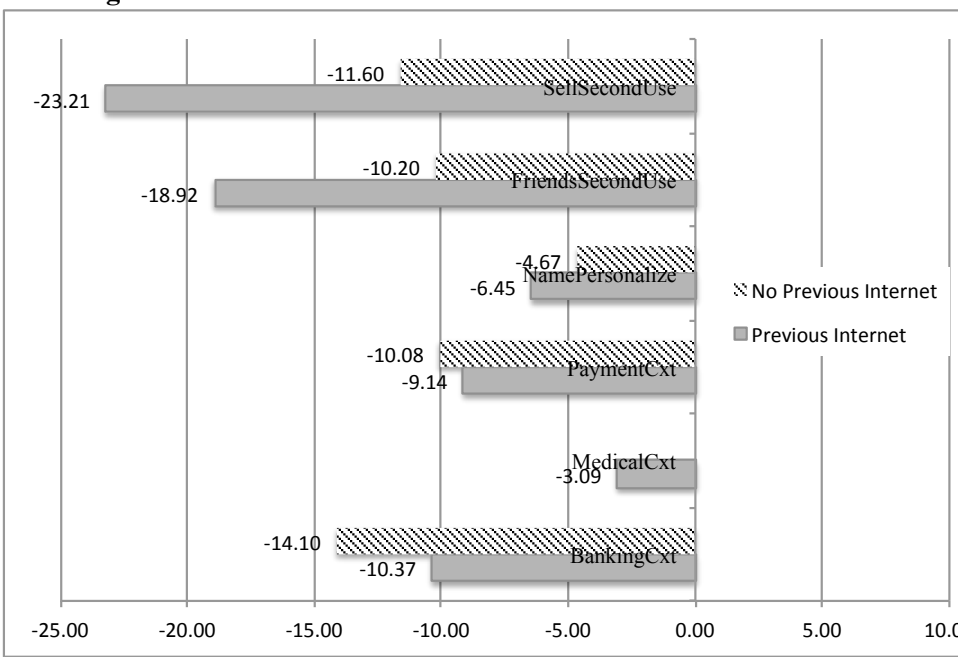


Figure 2: Relative Importance of Contextual Factors By Respondent Experience Online – Tracking Users Vignettes



5. IMPLICATIONS AND CONCLUSION

This study examined the factors that drive users' privacy expectations online. The results suggest that contextual factors significantly impact meeting privacy expectations. Yet, not all contextual factors – context, information, recipient, use – have equal weight in meeting or violating privacy expectations. Specifically the secondary use of information and personalized information have greater impact on privacy expectations. However, contextual factors do not explain the entire story as individual variances in privacy expectations persist, suggesting that both individual attitudes and contextual factors are important to examinations of privacy. Previous online experience is an important attribute impacting the importance of contextual factors for privacy expectations.

The findings speak to the relative importance of contextual factors to meeting privacy expectations rather than generalizing about the specific practices within the vignettes. Respondents were not given the name of a specific website, which could impact trust and perceived privacy violations. In addition, the vignettes offer hypothetical scenarios and the respondents were not actually at risk of a privacy violation. Such hypotheticals could suggest respondents would focus less on contextual factors and rely more on individual attributes, suggesting the results may be conservative in their measurement of the relative importance of contextual factors. However, the design does allow respondents to have full knowledge of the practices of the hypothetical firm through the vignette, thereby overcoming a limitation

in measuring users' privacy perceptions online and users' lack of knowledge of current tracking practices (Turow, Hennessy, & Draper, 2015).

5.1 Implications for Research

For researching privacy, this study demonstrated the utility of a highly contextualized examination of privacy judgments. The results illustrate the limits of general dispositions or attitudes in explaining particular privacy judgments online: respondents continued to take into account contextual factors in forming privacy judgments. However, this study also illustrates that relying *solely* on contextual factors to explain privacy expectations would miss the impact of individual variance in privacy judgments and in the relative importance of contextual factors. More work is needed to understand how individuals vary in their privacy equations both online and offline.

Users with less experience online – here, with no Internet access prior to joining the panel – have less certainty in their particular privacy judgments, self-describe with a lower privacy-is-important rating, trust websites less, yet find that tracking user scenarios meet privacy expectations *more* and place less importance on websites being in banking, medical, and social networking contexts. Taken together, the results appear to be consistent with a social contract approach to privacy – where insiders (those with more experience) would understand the privacy norms better, have greater trust in the institutions of their community, and take into account the contextual factors to a greater extent in their privacy judgments.

The results suggest that studying privacy should involve an understanding of individuals' disposition towards privacy and trust generally in addition to the contextual factors of a given situation. Focusing solely on individual differences ignores the important firm policies about how information is used, stored, and distributed in the degree to which specific scenarios meet privacy expectations. In addition, relying on privacy as contextually defined alone misses the individual variance, such as in a general privacy attitude or the degree of institutional trust, for privacy online.

This paper suggests definitions of privacy expectations that allow for both individual differences in attitude and interpretation and contextually dependent privacy norms offers a realistic path forward for scholars and researchers. More work should be done to extend the finding that online experience impacts how respondents assess contextual factors. Previous Internet access of respondents is a crude proxy for experience and more work could be done to identify how and when privacy norms converge on a context-dependent expectation. While detailed instruments exist to capture general privacy concerns, less work has been done to understand the type of online experience that impacts privacy expectations.

5.1.1 Privacy Paradox

The oft-reported privacy paradox, whereby individuals report a general belief that privacy is important yet continue to share information (Pavlou, 2011; Smith et al., 2011; Xu et al., 2011), could be explained if disclosing information is within the contextually defined privacy expectations. The results suggest users have fairly nuanced definitions of privacy expectations and retain expectations of privacy after disclosure: the paradox found in scholarship – of users raising privacy concerns and still disclosing information online – may not be a paradox for users.

The privacy paradox described could also be explained by users' learned helplessness or despondency (Egelman, 2013; Shklovski, Mainwaring, Skúladóttir, & Borgthorsson, 2014; Turow et al., 2015). Turow et al (2015) offers an alternative to the privacy tradeoff where consumers may be resigned to giving up data (Turow et al., 2015). Turow et al suggest consumers find data collection as something undesirable – as was found in the results here – yet inevitable (Turow et al., 2015, p. 13). Similarly, Shklovski et al (2014) find users move past privacy policies to download apps due to resignation to data collection tactics as "the way things are" (p. 2351). Other respondents *assumed* the data collection tactics were within the contextual norms of the application – this assumption is also found when online generally (Martin, 2015a). Upon finding out about the data collection practice, users felt either outrage or dejected acceptance (Shklovski et al., 2014).

Finally, Egelman (2013) investigates the privacy tradeoff and illustrates how habituation prevents respondents from understanding the differences between data collection policies; users familiar with a website did not fully engage with the privacy dialogs. This would suggest that greater experience could habituate users to the privacy interface and hinder them from understanding actual data collection and use practices, thus reinforcing the general implication of this study for further research on the types of general online experience important to privacy judgments and behavior.

5.1.2 Research Methods

All privacy research rests on a definition of privacy norms and expectations, whether explicitly mentioned or implicitly assumed. Concern around a specific practice or norm assumes that the practice is important and desirable expectation. By exploring whether and how privacy norms and expectations differ across contexts *and* individuals, this study has attempted to offer an inductive analysis into the definition of privacy. Future research could examine how varying the privacy expectations across individuals and contexts impacts privacy measurements such as a concern for privacy or a valuation of privacy.

Privacy expectations need not be static over time and more work could be done to examine how privacy norms and expectations can evolve or be influenced. Longitudinal studies of privacy expectations

evolving over time may be able to identify how privacy norms converge on a form of reflective equilibrium (Rawls, 2009). For example, individuals may begin to converge onto settled norms over time, thereby erasing differences in judgments attributable to individuals. In addition, a social contract approach to privacy would support greater agreement about a context-dependent definition of privacy expectations with insiders or contractors.

In addition, the Appendix includes a comparison of the theoretical generalizations for each of the samples: the nationally representative sample (GfK/Knowledge Networks), Amazon Mechanical Turk, and undergraduate students. The results suggest that Amazon Mechanical Turk provides a valid substitute for professional, large-scale samples for theoretically generalizable results. Unfortunately, the findings suggest the limited generalizability for student samples, which should be judged only as speaking to a larger audience of students and not necessarily to an adult population; the privacy equations based on the student sample and the nationally representative sample differ significantly.

5.2 Implications for Practice

For firms and managers, the results suggest that the secondary use of consumer information – as a general contextual factor included in the theoretical framework of privacy expectations – is a primary driver of websites not meeting privacy expectations of respondents. While much attention is made of 'sensitive' information, the type of general information initially gathered was not an important factor in meeting privacy expectations. For firms, what information is gathered may not be as important as how the data is then used, stored, and distributed. The findings here reinforce Bansal and Zahedi's (Bansal & Zahedi, 2015) results that unauthorized sharing is more problematic to user trust than a security violation.

Based on the findings reported here, firms have more options to meet the privacy expectations of users. Privacy norms and expectations may be malleable by educating users on the need for the information practice or allowing users a chance to experience the website or application. Rather than fixing a judgment of a privacy violation, firms would avoid a privacy violation altogether by bringing users' privacy expectations and firm policies into alignment.

5.3 Limitations

The factorial vignette methodology offers hypothetical scenarios and provides a bridge between experiments and surveys (Wallander, 2009); and the methodology also carries the strengths and weaknesses of both types of empirical work. The methodology captures the complexities of real decision making, and the highly controlled nature of the vignettes promotes greater internal validity than in usual

surveys. In addition, since changes in the vignettes are subtle, respondents are less susceptible to social desirability bias as in conventional surveys (Taylor, 2006; Wallander, 2009) – an important point when studying privacy and normative judgments in general.

However, the contributions discussed above should be interpreted within the context of a hypothetical quasi-experimental survey methodology which may not identify the 'real' reason the respondents judged the vignettes to meet (or not meet) their privacy expectations (Taylor 2006). In the study's design, researcher bias can influence the inclusion of factors, and missing factors could change the final models. Finally, the results point to the attitudes of the respondents rather than their expected behavior. Additional research would be required to parse the possible responses to firms' meeting or violating privacy expectations. The lack of a brand name and the general measurement for online experience also contribute to the limited ecological generalizability of the results. More work should be done to explore the impact of experience and the type of experience important to privacy judgments.

5.4 Conclusion

This study can be seen as a first step to address the need for a more precise measurement of information privacy by inductively identifying the privacy expectations of users online. Understanding the drivers of users' privacy expectations online should enable practitioners to respect privacy expectations of consumers and support researchers in related measurements such as privacy concerns, valuations, and protection responses. Importantly for research and practice, studying privacy should involve not only an understanding of individuals' general disposition towards privacy and trust but also a website's specific practices about the collection and use of information. More work should be done to inductively explore what the privacy expectations are for a given context and group of uses before asking if individuals are concerned with or value that expectation of privacy.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*, 509–514.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook (pp. 36–58). Presented at the Privacy enhancing technologies, Springer.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*, 160–174.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*, 249–274.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*, 339–370.

Anton, A., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *Security & Privacy, IEEE*, *8*, 21–27.

Auspurg, K., Hinz, T., Liebig, S., & Sauer, C. (2014). The Factorial Survey as a Method for Measuring Sensitive Issues. In U. Engel, B. Jann, P. Lynn, A. Scherpenzeel, & P. Sturgis (Eds.), *Improving Survey Methods: Lessons from Recent Research* (pp. 137–149). Taylor & Francis.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*, 138–150.

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62–77.

Beales, J. H., & Muris, T. J. (2008). Choice or consequences: Protecting privacy in commercial information. *The University of Chicago Law Review*, 109–135.

Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods*, *43*, 800–813.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*, 1017–1042.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal*, *25*, 573–578.

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012a). Evaluating online labor markets for experimental research: Amazon. com's Mechanical Turk. *Political Analysis*, *20*, 351–368.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012b). Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk. *Political Analysis*, *20*, 351–368.

Boulding, W., Kalra, A., Staelin, R., & ZEITHAML, V. A. (1993). A Dynamic Process Model of Sevice Quality: From Expectations to Behavioral Intentions. *Journal of Marketing Research*, *30*, 7–27.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, 47–70.

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*, 323–342.

Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*, 61–80.

Dinev, T., & Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*, 7–29.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, *46*, 81–83.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*, 877–886.

Egelman, S. (2013). My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect (pp. 2369–2378). Presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM.

Federal Trade Commission. (2010). *Protecting Consumer Privacy in an Era of Rapid Change*. FTC. Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

Federal Trade Commission. (2012). *FTC's Privacy Report: Balancing Privacy and Innovation*. FTC. Retrieved from http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report

Ganong, L. H., & Coleman, M. (2006). Multiple segment factorial vignette designs. *Journal of Marriage and Family*, *68*, 455–468.

Gefen, D., & Pavlou, P. A. (2012). The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research*, *23*, 940–959.

Grossklags, J., & Acquisti, A. (2007). When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. Presented at the WEIS.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks (pp. 71–80). Presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, ACM.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2008). Consumer privacy and marketing avoidance: A static model. *Management Science*, *54*, 1094–1103.

Harris Interactive. (2003). Most people are "privacy pragmatists" who, while concerned about privacy, will sometimes trade it off for other benefits. *The Harris Poll*, *17*, 44.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*, 275–298.

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's Privacy Homo Economicus. *Wake Forest L. Rev.*, *49*, 261.

Horrigan, J. (2013). *Broadband Adoption and Use in America*. FCC. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf

Horton, J. J., Rand, D. G., & Zeckhauser, R. J. (2011). The online laboratory: Conducting experiments in a real labor market. *Experimental Economics*, *14*, 399–425.

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research*, *34*, 334–423.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, *24*, 579–595.

John, L. K., Acquisti, A., & Loewenstein, G. (2011a). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*, 858–873.

John, L. K., Acquisti, A., & Loewenstein, G. (2011b). Strangers on a plane: context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*, 858–873.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*, 607–635.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*, 637–667.

Kugler, M. B., & Strahilevitz, L. (2015). Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory. *University of Chicago Public Law & Legal Theory Working Paper*, *534*.

Lanier, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review*, *12*, 1–45.

Lease, M., Hullman, J., Bigham, J., Bernstein, M., Kim, J., Lasecki, W., … Miller, R. (n.d.). *Mechanical Turk is Not Anonymous* (SSRN Scholarly Paper No. ID 2228728). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2228728

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*, 62–71.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*, 434–445.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing (pp. 501–510). Presented at the Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ACM.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*, 471–481.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354.

Madden, M., & Rainie, L. (2002). *America's Online Pursuits*. Pew Research Center. Retrieved from http://www.pewinternet.org/2003/12/22/part-3-information-utility-activities/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research*, *15*, 336–355.

Martin, K. (2012a). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*, *111*, 519–539.

Martin, K. (2012b). Information technology and privacy: conceptual muddles or privacy vacuums? *Ethics and Information Technology*, *14*, 267–284.

Martin, K. (2015a). Privacy Notices as Tabula Rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, *34*, 210–227.

Martin, K. (2015b). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 1–19.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*, 1–23.

Milne, G. R., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. *Journal of Public Policy & Marketing*, *29*, 138–149.

Mulligan, D. K., & King, J. (2011). Bridging the gap between privacy and design. *U. Pa. J. Const. L.*, *14*, 989.

Nguyen, D. H., Bedford, A., Bretana, A. G., & Hayes, G. R. (2011). Situating the concern for information privacy through an empirical study of responses to video recording (pp. 3207–3216). Presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*, 32–48.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 100–126.

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go. *MIS Quarterly*, *35*, 977–988.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly*, 105–136.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*, 27–41.

Ravichandran, R., Benisch, M., Kelley, P. G., & Sadeh, N. M. (2009). Capturing social networking privacy preferences (pp. 1–18). Presented at the Privacy Enhancing Technologies, Springer.

Rawls, J. (2009). *A theory of justice*. Cambridge, MA: Harvard University Press.

Rossi, P. H., & Nock, S. L. (1982). *Measuring social judgments: The factorial survey approach*. Sage Beverly Hills, CA.

Ross, J., Irani, L., Silberman, M. S., Zaldivar, A., & Tomlinson, B. (2010). Who are the crowdworkers?: shifting demographics in mechanical turk. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems* (pp. 2863–2872). New York, NY, USA: ACM.

Schreiner, M., & Hess, T. (2015). Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies. *ECIS Completed Research Papers*, *164*.

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management*, *50*, 1–12.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use (pp. 2347–2356). Presented at the Proceedings of the 32nd annual ACM conference on Human factors in computing systems, ACM.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*, 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996a). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996b). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 477–564.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 503–529.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *Software Engineering, IEEE Transactions on*, *35*, 67–82.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of Privacy and Confidentiality*, *4*, 2.

Sultan, F., & Rohm, A. J. (2004). The evolving role of the internet in marketing strategy: an exploratory study. *Journal of Interactive Marketing*, *18*, 6–19.

Taylor, B. J. (2006). Factorial surveys: Using vignettes to study professional judgement. *British Journal of Social Work*, *36*, 1187–1207.

Toch, E., Cranshaw, J., Drielsma, P. H., Tsai, J. Y., Kelley, P. G., Springfield, J., … Sadeh, N. (2010). Empirical models of privacy in location sharing (pp. 129–138). Presented at the Proceedings of the 12th ACM international conference on Ubiquitous computing, ACM.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*, 254–268.

Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation* (pp. 1–24). Annenburg School of Communication. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Van de Hoven, J. (2008). Information technology, privacy, and the protection of personal data. *Information Technology and Moral Philosophy*, 301–321.

Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*, 415–444.

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research*, *38*, 505–520.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*, 63–70.

Wang, N., Wisniewski, P., Xu, H., & Grossklags, J. (2014). Designing the default privacy settings for facebook applications (pp. 249–252). Presented at the Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing, ACM.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193–220.

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

Westin, A. Opinion surveys: What consumers have to say about information privacy, § The House Committee on Energy and Commerce, W.J. Billy Tauzin, Chairman (2001).

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*, 431–453.

Xu, H., Crossler, R. E., & Bélanger, F. (2012). A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems*, *54*, 424–433.

Xu, H., Luo, X. R., Carroll, J. M., & Rossen, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*, 42–52.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (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*, 1342–1363.

Xu, H., Wang, N., & Grossklags, J. (2012). Privacy by ReDesign: Alleviating Privacy Concerns for Third-Party Apps. *Thirty Third International Conference on Information Systems*.

Xu, H., Zhang, C., Shi, P., & Song, P. (2009). Exploring the role of overt vs. covert personalization strategy in privacy calculus. (Vol. 2009, pp. 1–6). Presented at the Academy of Management Proceedings, Academy of Management.

Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1993a). The nature and determinants of customer expectations of service. *Journal of the Academy of Marketing Science*, *21*, 1–12.

Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1993b). The nature and determinants of customer expectations of service. *Journal of the Academy of Marketing Science*, *21*, 1–12.

Zhang, F., Shih, F., & Weitzner, D. (2013). No surprises: measuring intrusiveness of smartphone applications by detecting objective context deviations (pp. 291–296). Presented at the Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society, ACM.

Measuring Privacy Expectations Online:

An empirical investigation into factors driving consumers' privacy judgments online

APPENDIX A

Comparing Results across National, Student, and MTurk Samples.

Both factorial vignette surveys reported in the article "Measuring Privacy Expectations Online: An empirical investigation into factors driving consumers' privacy judgments online" on targeted advertising and tracking users online were deployed to three different samples. The national sample was recruited via GfK/Knowledge Networks, which is an online research panel representative of the entire U.S. population. This national sample was used for the analysis and results in the main article. GfK/KnowledgeNetworks panel members are randomly recruited through probability-based sampling; households are provided access to the Internet and hardware if needed. This representative sample was gathered by GfK/Knowledge Networks by recruiting panel members with listed and unlisted telephone numbers, telephone and non-telephone households, and cell phone only households, as well as households with and without Internet access.[4]

For this study, GfK was subsidized via TimeSharing Experiments for the Social Sciences (TESS). TESS provides principal investigators access to a random, probability-based sample for online surveys using experimental design. One survey was accepted to the TimeSharing Experiments for the Social Sciences (TESS) program in their blind peer-reviewed selection process for a subsidized large, diverse population of research participants. The additional respondents (1200+) were paid for by the NSF grant.

Second, the surveys were piloted on Amazon Mechanical Turk (MTurk). 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.[5] Though use of Mechanical Turk for survey deployment has been criticized (Lease et al., n.d.; Ross, Irani, Silberman, Zaldivar, & Tomlinson, 2010), studies have shown that mTurk workers are more representative of the US population than the samples often used in social science research (Behrend, Sharek, Meade, & Wiebe, 2011; Berinsky, Huber, & Lenz,

[4] Only persons sampled through these probability-based techniques were eligible to participate on KnowledgePanel. Unless invited to do so as part of these national samples, no one on their own can volunteer to be on the panel. Documentation regarding KnowledgePanel sampling is available online at: http://www.knowledgenetworks.com/ganp/reviewer-info.html;

[5] For a full description, see Mason & Suri (Mason & Suri, 2012). For how MTurk samples are more representative of the U.S. population than in-person convenience samples, see Berinksy et al.,(Berinsky, Huber, & Lenz, 2012a). For the external and internal validity of MTurk, see Horton et al., (Horton, Rand, & Zeckhauser, 2011). In sum, respondent samples on MTurk are found to be representative of the general population with high internal and external validity. This analysis further supports this general finding.

2012b). The findings reported in this appendix will further validate the utility of MTurk as a research sample.

Third, the surveys were given to undergraduate students at a private, mid-Atlantic university's behavioral lab. Run through the school, the behavioral lab offers students partial credit for participation in the survey. Appendix A compares the composition and results of the three different samples. Table A1 contain a comparison of sample statistics of the three different samples for the targeted advertising survey.

Table A1: Comparing Sample Statistics for Targeted Advertising Survey

	For each comparison between Sample a v. Sample b: (t value, p value) Mean a v. Mean b		
	MTurk v. National	**MTurk v. Students**	**National v. Students**
Male	-2.3821, .0174 .5699 v. .5006	-4.0355, .0001 .5699 v. .4038	-2.4876, .0130 .5006 v. .4038
Age	13.9927, 0.00 34.8 v. 47.8	15.91, 0.00 34.8 v. 20.91	22.90, 0.00 47.8 v. 20.91
Privacy-is-Important Rating	-1.4252, .1543 72.831 v. 69.6573	.5415, .5884 72.8305 v. 74.3558	1.5703, .1167 69.6573 v. 74.3558
Trust-Sites Rating	-5.5397, 0.0 7.5424 v. -6.3235	1.6808, .0933 7.5424 v. 114.8317	2.4381, .0149 -6.3235 v. 114.8317
_eq2_R2	-3.8454, .0001 .7171 v. .6744	-5.6321, 0.0 .7171 v. .6325	-2.9370, .0034 .6744 v. .6325
DVMean (average rating)	-5.3850, 0.0 -16.9246 v. -29.1309	4.9453, 0.0 16.9246 v. -2.9237	8.8886, 0.0 -29.1309 v. -2.9237
DVsd (standard dev of dv)	-7.2846, 0.0 37.0962 v. 29.2563	-1.4656, .1432 37.0962 v. 34.9699	4.1705, 0.0 29.2563 v. 34.9699

Not surprisingly, the samples differed in composition. For the targeted advertising survey, the national sample was less male (50%) than the MTurk sample (57%) and older (48 years old versus 35 years old for MTurk). In addition, MTurk workers trust websites more (+7.54) in comparison to the national sample (-6.32). The average rating task for the national sample was also lower (-29.13) in comparison to the MTurk workers (-16.92). Interestingly, the privacy-is-important rating was statistically the same for both MTurk and the national sample. These trends held for the tracking users survey as well.

The relationships between these control variables, however, did not significantly differ between the national sample and MTurk workers. The role of four individual-level attributes on both the average rating task (DVMean) and the respondent-level R^2 was examined; R^2 measures the certainty of the individual's privacy judgment. Trust (+), privacy-is-important (-), age (-), and being male (+) had the same impact on the average rating task for national sample and MTurk workers for targeted advertising and tracking user surveys. Trust (+), privacy-is-important (+), age (+) and being male (-) also had the same impact on the respondent-level R^2 for both the national sample and MTurk for the targeted

advertising and all but age for the tracking users survey (age was not significant in the respondent-level R^2 for tracking users for the national sample).

While the level of expertise or experience of the respondents was *not* captured directly in any of the surveys, which is a limitation of the current study, GfK/Knowledge Networks does capture whether or not their respondents had Internet access prior to being included in the panel. This variable PPNET designates is if the respondent had prior Internet access and is a crude proxy for experience online: if a respondent did not have Internet access at home before becoming a member of GfK/Knowledge Network's panel, that respondent would have less experience online than a respondent that already had access. For both the targeted advertising and tracking users surveys, those respondents with less experience (no prior Internet access) believe privacy is less important, trust websites less, and are less certain in their privacy judgments than those with more experience. These results suggest that respondents in the national sample with prior experience behave similarly to the MTurk sample in the individual attributes such as trust in websites and the privacy-is-important rating. Interestingly, experience does not have as much of an impact on the rating task directly (DVMean), but does impact the privacy equation below.

Table A2 summarizes the multi-level regression analysis for each of the samples – including a break out of the national sample into those with and without prior internet access – and the results suggest that MTurk is a valid substitute for the national sample as explained below.

In sum, while the compositions of the samples differ, the generalizable results of the national sample and MTurk sample are consistent. Most importantly, the primary contextual factors and the importance of the individual control variables are statistically identical across the national sample and MTurk sample for both the tracking users and targeted advertising surveys. The top 5 drivers for both the national and MTurk samples are identical as summarized in Tables A2. Targeting survey results are shown in the interest of space. For both MTurk and the nationally representative sample, the top five drivers of privacy expectations for targeted advertising are the use of friends, names, payment context, banking context, and location information. For both MTurk and the nationally representative sample, in addition (while not shown) the top five drivers of privacy expectations around tracking users are the selling of information, using information to target friends, banking context, payment context, and names. The importance of the individual control variables is also identical across the national and MTurk sample.

Unfortunately, the student sample gives results with little in common to either the national sample or the MTurk sample—particularly for the targeted advertising vignettes. The analysis of the student sample would suggest a purely contextual definition of privacy and downplays the importance of difference in privacy judgments attributable to the individual. The privacy equation from the student sample contains very different contextual factors as included in Table A2. In addition, the intra-class

correlation coefficient, which measures the variation in the rating task attributable to the individual in this case, is significantly lower for the student sample (32-33%) in comparison to the national sample (55-57%) and the MTurk sample (42-43%) for both surveys.

These findings have limitations. The results are based on a web-based online survey that can be easily translated between sample settings. In addition, the subject of the survey is online judgments and expectations, so additional study is needed to identify if these samples perform similarly when the methods and subject are not online.

In sum, MTurk appears to provide a valid and economical substitute for nationally representative online surveys. Student samples should be generalized with care and, unless proven otherwise, to only a student population.

Table A2: Comparing Privacy Equations—Targeted Advertising Vignette Study**

	National Sample	**Mechanical Turk**	**Students** -	**National Sample NET Access** -	**National Sample No NET Access**
Control Variables					
Male					
Age	**-0.62**	**-0.62**		**-0.70**	
PPNET					
TrustSites	**0.27**	**0.28**		**0.24**	**0.35**
PrivacyImportant	**-0.23**	**-0.20**		**-0.23**	**-0.21**
_cons	**23.49**	**17.65**		**22.44**	**31.49**
Model Statistics					
N	31,160	18,760	8,320	24,880	6,280
ICC Model 0	57.0%	42.9%	32.8%	53.0%	60.6%
sd(_cons)	34.8	31.6	25.9	34.3	36.5
Deviance	309,850	192,758	84,388	247,311	62,422
df	27	27	27	27	27
Top 5 Drivers of Privacy Judgments					
	Friends	Friends	Friends	Friends	Friends
	Name	Name	Name	Name	Name
	Payment	Payment	Primary Ad	Payment	Payment
	Banking	Banking		Banking	News
	Location (+)	Location (+)		Location (+)	Banking
Model Statistics					
AIC	309903.9	192811.9	84441.69	247365.2	62476.25
BIC	310129.2	193023.6	84631.41	247584.5	62658.37
ICC	52.3%	38.9%	32.6%	51.5%	54.8%

*** bold = p < 0.05;** *regular = p < 0.01; blank = n.s*