Journal of Business Research 82 (2018) 103–116

Contents lists available at ScienceDirect

Journal of Business Research

journal homepage: www.elsevier.com/locate/jbusres

The penalty for privacy violations: How privacy violations impact trust online☆

Kirsten Martin

George Washington University, USA

ARTICLE INFO

Keywords:
Privacy
Online trust
Trust factors
Website trust
E-commerce

ABSTRACT

With information misuse as a particularly salient form of risk online, respecting privacy is often closely tied to trust in consumer surveys. This study uses factorial vignette survey methodology to measure the relative importance of violating privacy expectations to consumers' trust in a website. The findings suggest consumers find violations of privacy expectations, specifically the secondary uses of information, to diminish trust in a website. Firms that violate privacy expectations are penalized twice: violations of privacy (1) impact trust directly and (2) diminish the importance of trust factors such as integrity and ability on trust. In addition, consumers with greater technology savvy place greater importance on privacy factors than respondents with less knowledge. Violations of privacy may place firms in a downward trust spiral by decreasing not only trust in the website but also the impact of possible mechanisms to rebuild trust such as a firm's integrity and ability.

1. Introduction

Across context and industries, trust is important to maintain stakeholder relationships. Trust, as the willingness to accept vulnerability to the actions of another, has been found to be particularly important in situations with greater uncertainty, interdependence, and a fear of opportunism (Gefen, 2002; Mayer, Davis, & Schoorman, 1995a). Trust assuages the risk consumers perceive in regards to e-commerce (Gefen & Pavlou, 2012; Xu, Wang, & Teo, 2005) and is critical to users sharing information (Hoffman, Novak, & Peralta, 1999b) as well as the adoption of new technology (Miltgen, Henseler, Gelhard, & Popovič, 2016). When online, information risk persists as a source of vulnerability: who can use the information, for what purpose, and for how long? Information asymmetries and a lack of safeguards render online information exchanges fraught with greater uncertainty and a risk of opportunism (Martin, 2013).

With information as a particularly salient form of risk online, it is not surprising that meeting or violating privacy expectations is closely tied to trust by consumers (Pew Research Center, 2014; Turow, Hennessy, & Draper, 2015a). Privacy, as the norms and expectations of information flow within a context (Nissenbaum, 2010), governs how information should be treated. Respecting privacy means respecting the norms of what information is gathered, how information is used, and with whom information is shared; violating privacy means violating those information norms (Martin, 2016b; Nissenbaum, 2010). We have yet to understand how privacy violating behavior, behavior that violates the rules about how information should be gathered and for what purpose within a context, impacts consumer trust in a website. Privacy seals and notices have been used as a proxy for privacy in research, yet recent work has shown users have privacy expectations and identify privacy violations regardless of the presence or substance of the privacy policy (Martin, 2015a).

While research has detailed important trust factors impacting trust online, specifics as to the role of meeting or violating privacy expectations online on consumer trust has not been examined. For example, consumers' online trust factors have included details such as the influence of recommendation types (Smith, Menon, & Sivakumar, 2005), a website's ease of use (Awad & Ragowsky, 2008), a user's relationship to fellow posters (Pan & Chiou, 2011), website design (Urban, Amyx, & Lorenzon, 2009), a website's characteristics, order fulfillment, and absence of errors (Bart, Shankar, Sultan, & Urban, 2005), a website's reputation and communication (Mukherjee & Nath, 2003), and even the legalistic-nature of a notice (Pan & Zinkhan, 2006). Such detail gives specific prescriptions to maintain trust online as well as contextualizing theoretical trustworthy concepts such as ability and integrity. Violations of privacy expectations, on the other hand, are difficult to measure, highly contextual, and have not been included in such particularized examinations of trust. Since much of marketing online relies upon gathering, storing, aggregating, and sharing consumer information, whether these practices impact consumer trust is

☆ This material is based upon work supported by the National Science Foundation under Grant # 1311823 and Grant # 1649415. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

E-mail address: martink@gwu.edu.

http://dx.doi.org/10.1016/j.jbusres.2017.08.034
Received 28 June 2016; Received in revised form 29 August 2017; Accepted 31 August 2017

critical for firms online.

This paper contributes to understanding the drivers of trust in online exchanges and makes the explicit link between meeting or violating privacy expectations and consumer trust. Specifically, this paper examines the role of violations of privacy expectations on consumer trust judgments in a firm and how respondents vary in assessing violations of privacy expectations in trusting a firm. Using a factorial vignette survey, realistic online scenarios were rated by respondents to identify which factors were important to trusting a website. Three surveys were run to systematically include privacy factors, trust factors, and both privacy and trust factors in the vignettes in order to isolate the impact of privacy on trust.

The findings suggest consumers find violations of privacy – operationalized as the secondary uses of information to sell to a data aggregator and retarget ads to friends – to diminish trust in the website. Firms that violate privacy expectations are penalized twice –violations impact trust directly and diminish the importance of trust factors such as integrity and ability on trust. Finally, while consumers with a high concern for privacy and low trust in websites are less trustful of specific firms, consumers with greater technology savvy – greater knowledge of the Internet and coding experience – place greater importance on privacy factors than those not technology savvy.

2. Hypotheses development: privacy and trust

2.1. Models of privacy & trust

Trust has been defined as the willingness to accept vulnerability of an individual, group, organization, or institution (Mayer, Davis, & Schoorman, 1995b; Pirson, Martin, & Parmar, 2014). Trust is studied at (at least) three levels: (1) individuals have a propensity or disposition to trust generally (Mayer et al., 1995b; McKnight, Choudhury, & Kacmar, 2002), (2) individuals may trust in an institution such as congress, banking, or online (Pavlou & Gefen, 2004), and (3) individuals trust a particular individual or organization by taking into consideration the trustworthiness signals of the trustee such as ability, benevolence, and integrity (Gefen, 2002).

Privacy and trust have parallel levels of analysis with both general attitudes, beliefs, and dispositions as well as particular judgments about a person or firm. Pirson et al. (2014) distinguish specifically between institutional trust and stakeholder trust in a firm. Stakeholder trust – here focusing on consumer trust – is closer to personalized trust in that an individual is willing to accept vulnerability of the actions of a particular organization. As shown in Fig. 1 Arrow D, consumer trust is based on the trusting tendencies of the consumer (Bhattacherjee, 2002; Pavlou & Gefen, 2004) (McKnight et al., 2002) in addition to the ability, benevolence, and integrity of website or firm (Belanger, Hiller, & Smith, 2002).

In parallel, consumers have a general privacy disposition that transcends particulars of a situation. Similar to trust judgments about a website, privacy judgments are a combination of individual dispositions or attitudes about as well as contextual privacy factors around the type of information, context of use, and uses of information as shown in Fig. 1 Arrow E (Malhotra, Kim, & Agarwal, 2004; Martin & Shilton, 2015; Nissenbaum, 2010).

The goal of the review in Fig. 1 and Table 1 is to illustrate that the examination of the relationship between privacy and trust has focused on a general privacy concern of individuals or proxies for privacy violations partly because the empirical examination of context-dependent privacy definitions is relatively recent and partly because the actual information practices of a firm are not known by the consumer. What data is collected and how the data is used is not clear to consumers, so measuring how important such practices are is difficult in the field. Importantly, previous work linking privacy and trust has remained at the general level where consumers' general privacy valuation or concern impacts trust perceptions (Table 1 and Fig. 1 Arrow A). In parallel, trust disposition or institutional trust is found to reduce concerns about privacy (Rohm & Milne, 2004a; Xu et al., 2005) as in Fig. 1, Arrow B, and both general trust dispositions and privacy valuations jointly impact consumer intent and behavior (Arrow C).

While specific drivers of trust are examined, contextual approaches to privacy are difficult to empirically measure. Proxies – such as the existence of a seal or notice – are useful as a stand-in to respecting or violating privacy, where the presence of a seal is perceived as respecting privacy and the absence of a seal could be a violation of privacy. This study shifts to examine contextual definitions of privacy – such as privacy as contextual integrity (Nissenbaum, 2010, 2011) or a social contract approach to privacy (Martin, 2016) as shown in Arrow F. The focus of this study is the role of respecting versus violating privacy expectations in highly particular stakeholder trust in a firm – specifically the consumer trust in a particular website. The hypotheses below center on the role of violations of privacy expectations on consumer trust in a firm (H_1) and the role of violations of privacy expectations on the importance of trust factors on consumer trust (H_2) as well as how individual's differ in the importance of privacy violations on user trust (H_3 and H_4).

2.2. Role of violations of privacy expectations on trust judgments

Recent work on privacy suggests that privacy norms can be viewed

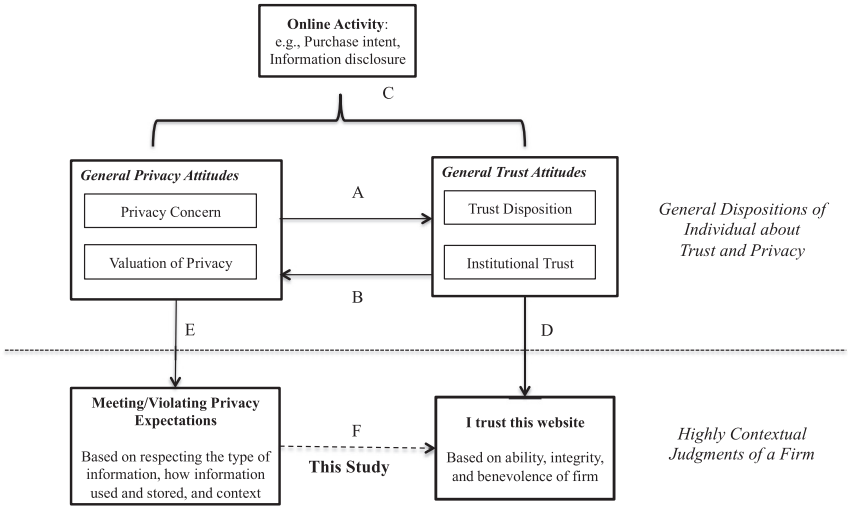

Fig. 1. Known relationships between privacy and trust (Table 1 includes references).

Table 1
Privacy and trust literature.

User general privacy disposition as antecedent to trust (Fig. 1 arrow A)	• General privacy concerns as an individual-level disposition can impact trust online (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). • Privacy disposition is an antecedent to trust in ecommerce (D. J. Kim, Ferrin, & Rao, 2008) • Disposition to trust and privacy concerns impact on trust in website through perception of risk (Thiesse, 2007). • Perceived privacy and security impacts general online trust (Riquelme & Román, 2014)) • General concern for privacy as impacting trust (Culnan & Armstrong, 1999; Metzger, 2004): • Increases in individuals' concern for information privacy is associated with registering for websites less frequently and providing incomplete information – perhaps due to decreased trust (Metzger, 2004; Sheehan & Hoy, 2000).
User institutional trust as impacting privacy judgments (Fig. 1 arrow B)	• Trust as important to reduce privacy risk (Xu et al., 2005). • Disclosure within a social contract contingent upon trust (Hoffman, Novak, & Peralta, 1999a; McKnight et al., 2002; Xu et al., 2005). • Greater trust in a firm leads to fewer concerns about privacy (Rohm & Milne, 2004b).
Privacy and trust attitudes as jointly important to intent and behavior (Fig. 1 arrow C)	• Trust and privacy as jointly important to judgments online (Schofield & Joinson, 2008) and for technology acceptance (Miltgen et al., 2016) • Effect of privacy concerns on behavioral intentions mediated by trust (Malhotra et al., 2004); trust in firm as moderating privacy concerns and ad click through (Bleier & Eisenbeiss, 2015). • Intent to use services influenced by trust and concern for privacy (Cases, Fournier, Dubois, & Tanner, 2010; Chellappa & Sin, 2005; Eastlick, Lotz, & Warrington, 2006). Privacy concerns as a moderator on the impact of trust on online purchase attitude (McCole, Ramsey, & Williams, 2010a). • Evidence of both a moderating and mediating relationship such that high privacy compensates for low trustworthiness and high trustworthiness compensates for low privacy on disclosure behavior (Joinson, Reips, Buchanan, & Schofield, 2010).
User institutional trust as impacting trust in firm (Fig. 1 arrow D)	• E.g., Institutional trust as impacting user trust in a firm (Bhattacherjee, 2002; Pavlou & Gefen, 2004).
User privacy disposition as impacting contextual privacy judgment (Fig. 1 arrow E)	• E.g., Consumers' privacy disposition as impacting contextual privacy judgments in mobile space (Martin & Shilton, 2015). Consumers' privacy disposition and privacy concern as impacting contextual privacy judgments about secondary use of information online (Martin, 2015a).
Meeting contextual privacy expectations as important to trust in a firm (arrow F: this study)	Studied here: Whether and how violating (or meeting) privacy expectations impacts user trust in a firm. Closest Measurement: • Seals are important (Lim et al., 2006) (Bart et al., 2005; Belanger et al., 2002; Hu, Wu, Wu, & Zhang, 2010; Lee & Turban, 2001), • Privacy notices (Bhattacherjee, 2002; Everard & Galletta, 2005; Mukherjee & Nath, 2007; Shankar et al., 2002) • FIPS as signal of trust (Hoffmann et al., 2014)

as sustainable agreements about what information is gathered, who has access to the information, and how information is used within a community (Martin, 2015b) or context (Nissenbaum, 2010). Privacy as a social contract – a mutually beneficial agreement within a community about sharing and using information –suggests that respecting privacy entails understanding the implicit privacy norms about what, why, and to whom information is shared within specific relationship or community. These social contracts are the stated and unstated agreements that individuals and groups make in contexts, communities, and relationships. Individuals within a particular community, such as teams or young adults or mobile app users, develop substantive privacy norms not easily recognized or understood by outsiders (Martin, 2012; Martin & Shilton, 2015; Turow, King, Hoofnagle, Bleakley, & Hennessy, 2009). Online, these privacy norms and expectations form an informal contract over privacy that can be either respected or violated; violations of privacy are when the appropriate norms are broken.

Meeting or violating users' highly contextual privacy expectations can be viewed as an antecedent to trust. Individuals are more willing to transact, and with greater frequency, if they perceive lower risk through on an understanding of the "rules of transaction conduct" (Gefen & Pavlou, 2012). And, privacy norms and expectations are an important "rule of conduct" online: individuals take into consideration contextual factors of privacy in making privacy judgments and these rules about privacy govern the expectations of how information will be gathered and used (Martin, 2015b; Martin & Shilton, 2015; Nissenbaum, 2010). Specifically, firms can violate consumers' privacy by not respecting the rules about the type of information gathered, how the information is used, and who has access to the information. These three privacy factors – what information is given to whom and for what purpose – work in tandem to create a contextual norm; breaking that norm constitutes a privacy violation. For example, location information is appropriate for map applications but not for flashlight applications (Martin & Shilton, 2015).

Respecting informal contracts has a clear positive relationship with trust, since empirical work generally shows that relational governance is positively associated with trust (Poppo & Zenger, 2002), while violating privacy expectations of users will negatively impact their trust in the website. Violations that contribute to the vulnerability of the user – such as changing who has access to the information – will constitute a violation of trust.

H_1. The presence of a violation of privacy expectations will decrease the user's trust in a website, all else being equal.

Users' trust judgments are based not only on their trust disposition or institutional trust, but also on the firm's perceived trustworthiness evidenced by their ability, benevolence, and integrity (Mayer et al., 1995b). Research suggests that breaches of agreements – even informal agreements – are a matter of breaking a promise and could, therefore, leave a user less impressed with other integrity signals of the firm in influencing trust. Further, ability if seen as mismanagement and competence, is a matter of both technological and managerial competence (Pirson et al., 2014) and the mismanagement of information could similarly leave users less focused on other ability signals. We therefore would predict Hypothesis 2.

H_2. The presence of a violation of privacy expectations will decrease the importance of trust factors on user's trust in a website.

2.3. How consumers differ in the importance of privacy for trust

In both the examination of privacy and trust, two individual-level factors have proven important. First, users have a general valuation of or concern about privacy and trust that transcends particulars of a situation. Privacy scholars include individuals' general privacy concern and privacy valuation as an important predictor as to how an individual will judge a situation and behave (Malhotra et al., 2004;

Martin & Shilton, 2015; Smith, Milberg, & Burke, 1996). Similarly, an individual's trust disposition and trust in an institution impacts their trust in a particular person or firm (e.g., Arrow D Fig. 1. Further, these privacy and trust measurements are related: Turow et al., 2015a conceptualize privacy despair as where individuals have high privacy concerns and valuations but little trust that companies will respect their privacy expectations. We would expect consumers who profess to have a greater privacy despair – greater concern about and valuation of privacy and less institutional trust – to place greater emphasis on violations of privacy expectations in forming trust judgments.

In addition, research has shown that technological experience and online knowledge is important to trust and trust increases due to the effects of familiarity (Gefen, 2002; Pavlou & Gefen, 2004). In addition, privacy expectations are an important set of norms online, and insiders have a better understanding of the privacy norms compared to outsiders of a community based on social contract theory (Martin, 2012). For consumers online, experience is a broad term (Gefen, Karahanna, & Straub, 2003; Lim, Sia, Lee, & Benbasat, 2006; Pavlou & Dimoka, 2006; Pavlou & Gefen, 2004) and can include technological competence and orientation (Mukherjee & Nath, 2003) as well as experience and internet savvy (Bart et al., 2005; Shankar, Urban, & Sultan, 2002). In general, we would expect consumers with greater experience – here, technological experience and Internet knowledge – to have a better understanding of the privacy expectations and to place greater emphasis on privacy violations in forming trust judgments.

H_3. Consumers who have a greater concern about and valuation of privacy place greater emphasis on prisvacy violations in forming trust judgments.

H_4. Consumers with greater technological experience or online knowledge will place a greater weight on privacy violations in making trust judgments.

3. Research methods

The hypotheses include both general dispositions about trust and privacy as well as the highly contextual privacy expectations and consumer trust judgments about a firm. Where the former is best gathered with traditional survey methodology, the latter requires varying the contextual factors of privacy (i.e., the type of information, how it is used, the context, etc) as well as trust (ability, benevolence, and integrity). The factorial vignette survey methodology in combination with traditional survey methodology was used to capture both types of judgments.

Factorial vignette survey methodology was developed to investigate human judgments using highly contextual vignettes (Jasso, 2006; Rossi & Nock, 1982; Wallander, 2009). In a factorial vignette survey, a set of vignettes describing hypothetical situations is generated for each respondent. Within the hypothetical situations, the attributes (factors) vary systematically in their value (levels) (Jasso, 2006). The goal is to identify how each factor impacts the respondents' evaluations (Sauer, Auspurg, Hinz, & Liebig, 2011). In this study, the survey asked respondents the degree to which the respondents' trusted the website described in the vignette, and statistical techniques were used to identify the relative importance of each vignette factor in driving the respondents' outcome (trust in a website).

Scenario-based surveys – to include conjoint analysis, vignette surveys, and factorial vignette survey methodology (FVSM) – are particularly useful to study how humans make multi dimensional judgments and choices (Hainmuellera, Hangartnerb, & Yamamotod, 2015). Vignettes have been used in surveys generally where a respondent would be given a single vignette and asked a series of survey questions about that vignette. Here, respondents are given the same rating task over a series of vignettes and later analysis will identify which factors influenced the judgment of respondents positively and negatively. The FVSM was created to capture multifaceted judgments indirectly by presenting respondents with stimuli that resembles real-world evaluations and asking them to make trade-offs between several dimensions with a single rating (Auspurg, Hinz, Liebig, & Sauer, 2014). As such, the FVSM, similar to conjoint analysis, 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 deciding to trust a firm, are notoriously difficult to examine as respondents may attempt to bias answers 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 trust judgments as well as differences across subgroups of consumers (Auspurg et al., 2014) which is theoretically suggested above.

Importantly, the factorial vignette survey methodology captures the relative importance of contextual factors for respondents. This enables the direct comparison of the relative importance of the trustworthiness of the website – ability, benevolence, and integrity – compared to and possibly moderated by the importance of specific violations of privacy to trust in a website. Here, a series three factorial vignette surveys were run to measure whether and how violations of privacy expectations impact a firm's trust and trustworthiness.

When designing a factorial vignette survey, the cognitive load on respondents is based on the complexity of the vignettes (factors and levels), the number of vignettes assigned to each respondent, and the rating task assigned to each vignette. These work in tandem to create an overall demand on the respondent. The factorial vignette survey methodology uses a single rating task but assigns respondents a larger number of vignettes ($10 - 110$) (Sauer et al., 2011). The design of the vignettes (factors and levels) and the number of vignettes per respondent is a balance between the statistical needs of the researcher and the cognitive load required for a single respondent to take the survey. As noted by Jasso (2006), the number of vignettes must be "large enough to enable precise estimation of respondent-specific equation yet small enough to prevent respondent fatigue." The respondent rated 40 such vignettes (taking approximately 10–12 min) for each of the three surveys run as described in Table 2.

3.1. Independent variables (vignette factors)

3.1.1. Privacy factors

In order to systematically vary the degree to which the hypothetical website met or violated privacy expectations, a series of independent variables based on contextual approaches to privacy were tested (Martin, 2015b; Nissenbaum, 2010)[1]: the context of the website (Cranor, Reagle, & Ackerman, 2000; Earp & Baumer, 2003; Nissenbaum, 2010), the type of information gathered (Cranor et al., 2000; Earp & Baumer, 2003; John, Acquisti, & Loewenstein, 2011; Malhotra et al., 2004; Martin & Shilton, 2015), and the primary and secondary use of information (Anton, Earp, & Young, 2010; Cranor et al., 2000; Martin, 2015a). The levels of each factor were chosen based on previous research and common practices online (gathering history of websites and location information; selling data to data aggregator; etc). Table 2 includes all the privacy factors and each level.

3.1.2. Trust factors

For Surveys 2 and 3, the vignettes include the trust factors ability, benevolence and integrity that have been shown to impact user trust (Bhattacherjee, 2002; Gefen et al., 2003; Gefen, Benbasat, & Pavlou,

[1] Separately, a survey was run to verify the vignette factors and levels included a proper range of privacy violating and exceeding behaviors. The same factors were included in a factorial vignette survey with the rating "This website met my privacy expectations." The results are listed as Survey 0 and Appendix A.

Table 2
Vignette factors.

	Factor	Operationalized in vignette
Privacy factors (Survey 1 & 3)	Information	Your gender and age Your current location information The history of websites you visited Only information you voluntarily provide
	Primary use	Provide a faster and more user-friendly website Tailor services for you Offer you discounts Place advertising targeted to you
	Storage	Only this current session, 1 month, 1 year, 5 years, 10 years
	Secondary use:	{null} May conduct research experiments using you and other users Sell to tracking company who combines the data with your other activities, Sends advertising to friends and contacts, Removes your name from the data and uses the data to improve their service.
Trust factors (Survey 2 & 3)	Ability	The website scores high on competence and effectiveness and always continuously improves their service [*Very high, high, average, low, very low*]
	Benevolence	The website always gives back to their local community. [*Always, usually, sometimes, rarely, never*]
	Integrity	The website is considered very honest and sincere in its dealings with customers, employees, and suppliers. [*extremely, very, moderately, slightly, not at all*]

Table 3
Sample vignette narratives – underline portion factor with multiple levels.

Survey	Template	Example with values
Survey 1–3	*A [CONTEXT] website silently collects [INFORMATION].*	A travel website silently collects the history of websites you visited.
Survey 2 & 3	*The [CONTEXT] site* *Scores [ABITLITY] and [ABITLITY] improves their service,* *Is considered [INTEGRITY] in its dealings with customers, employees, and suppliers,* *And [BENEVOLENCE] gives back to their local community.*	The travel site Scores very low on competence and effectiveness and never improves their service, Is considered somewhat honest and sincere in its dealings with customers, employees, and suppliers, And occasionally gives back to their local community.
Survey 1 & 3	*The [CONTEXT] site uses the data to [PRIMARY USE] and stores the data for [STORAGE].* [*SECONDARY USE*]	The travel site uses the data to provide a faster and more user-friendly website and stores the data for 10 years. The site removes your name from the data and uses the data to improve their service

2008; Hoffmann, Lutz, & Meckel, 2014; Lim et al., 2006). For the firm's ability, the website's competence and effectiveness varied; for benevolence, the firm's propensity to give back to their community varied from always to never; for integrity, the firm's honest and sincerity with stakeholder was varied. Table 2 includes both the privacy and trust factors included as well as how each was operationalized.[2] The factors were combined to form a vignette as shown below and in Table 3.

3.2. Rating task

The focus of this study is the highly particular stakeholder trust in a firm – specifically the consumer trust in a particular website. FVSM uses a single rating task across multiple vignettes (Auspurg et al., 2014; Jasso, 2006; Wallander, 2009).[3] 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. For each vignette, respondents were instructed: "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'." Respondents rated their agreement with the following prompt for each vignette: "I trust this website".

3.3. Respondent controls

Before and after the vignettes, the instrument supplied respondents with several questions to compare respondents. Respondents' age and gender were collected before the vignettes and the privacy, experience, and trust controls described below were asked after the vignettes to avoid priming the respondents. See Table A1 in the Appendix for the control variables included.

To test Hypothesis 3 based on the correlation of respondent factors, the respondents' knowledge of the Internet and coding experience was gathered as well as their general trust and privacy measures. For example, the respondents were asked to rate on a scale from 'strongly disagree' to 'strongly agree' their agreement with the statement: "In general, I trust websites." This rating captured respondents' institutional trust online. The second rating task asked for their agreement with the statement, "In general, I believe privacy is important." This rating captured respondents' general privacy belief.

Based on Hypothesis 3 and 4 as well as the correlation of respondent factors, an exploratory factor analysis was performed, and the results are in included in Appendix C. The factor analysis resulted in two

[2] While all three trust factors were included, benevolence had a smaller role in the respondents' trust judgments. The analysis focuses on the interaction between ability and integrity and the privacy violations. Interestingly, some trust scholars have focused on 'competence' (ability) and 'character' (integrity) as the primary trust factors driving trust in a firm and these results support that move (Elsbach & Currall, 2012; P. H. Kim, Ferrin, Cooper, & Dirks, 2004; Pirson et al., 2015).

[3] See also Rossiter (Rossiter, 2002) on single item measures as well as Schumann et al. (2014) on the tension in marketing literature around single item measures. The factorial vignette survey methodology relies upon a single item rating with multiple factors in the vignette to capture the complexity of the phenomenon. Multiple item measures for each of the 40 vignettes is considered invalid for the method (Jasso, 2006). However, if more than one rating task is needed, the preferred method is to run the survey experiment twice – once for each different rating task. This also keeps the cognitive burden lower.

distinct respondent-factors: a 'technology savvy' (TechSavvy) factor that is positively related to both coding experience and Internet knowledge and a 'Privacy Despair' factor which is positively related to a respondent's privacy concern and privacy valuation (privacy-is-important score) and negatively related to a respondent's trust in websites and trust disposition. The overall score for each respondent was calculated based on the weighted importance form the factor analysis.[4] In addition, the scores were broken into quartiles and respondent's quartile for each score was assigned (a respondent in the highest quartile for PrivacyDespair would be assigned a 3 on a scale from 0 to 3).

3.4. Sample

The surveys were deployed over the course of 3 months through Amazon's Mechanical Turk – a crowdsourcing marketplace where researchers publish a job ("HIT") for respondents to take a survey.[5] Respondents were paid $2 per completed survey and the surveys were run 2–3 weeks apart. Each survey had respondents rate 40 vignettes as shown in Table 4. Respondents were paid $2/survey and surveys were posted at 12 noon EST to capture all of the continental U.S. The descriptive statistics were consistent across survey runs.[6]

3.5. Analysis

The factorial vignette methodology creates a unique dataset with 40 judgments or ratings for each respondent. The resulting data set can be thought of in two levels: the vignette contextual factors and the respondent control variables. If *J* vignettes are nested within *I* individuals, then *I* is the number of the respondents with level 2 individual variables and *J* is the number of vignettes answered with level 1 factor variables, the general equation is:

$$Y_{ij} = \beta_0 + \Sigma\beta_k V_{jk} + \Sigma\gamma_h R_{hi} + u_i + e_j$$

where Y_{ij} is the rating of vignette *j* by respondent *i*, V_{jk} is the k^{th} factor of vignette *j*, R_{hi} is the h^{th} characteristic of respondent *i*, β_0 is a constant term, β_k and γ_h are regression coefficients for *k* vignette factors and *h* respondent factors, u_i is a respondent-level residual (random effect), and e_j is a vignette-level residual. The model conceptualizes the ratings as a function of the contextual factors described in the vignette (ΣV_k) and the characteristics of the respondent (ΣR_h) as hypothesized above.

Since the data can be modeled at two levels – the vignettes and the individual respondents – multi-level modeling was used to control for and measure individual variation in trust judgments. Multi-level modeling (xtmixed in STATA) accounts for the possibility that the error terms were not equal across individuals, and, later in the post-hoc analysis, that the intercepts and coefficients may vary across respondents with random intercept and random slope models.

Finally, a respondent-specific equation (Jasso, 2006) was developed by regressing the trust rating task on to the vignette factors for each respondent ($N = 40$). A new data set was formed for each survey with a trust equation for each respondent. The respondent-specific equation includes the respondent's intercept, the relative weight for each contextual factor, and a respondent-specific R^2 (Respondent R2 in Table 4) as in the equation below.

[4] TechSavvy = 0.643 ∗ KnowInternet + 0.5727 ∗ CodingExp;
PrivacyDespair = 0.6626 ∗ PrivacyConcern − 0.7677 ∗ TrustSites
+ 0.444 ∗ PrivacyImportant − 0.4305 ∗ TrustDisposition

[5] Turk has been used for consumer perceptions in marketing (Goldstein, Suri, McAfee, Ekstrand-Abueg, & Diaz, 2014; Yang & Lynn, 2014). In addition, a recent survey replicates (and extends) a Pew Research Study (Pew Research Center, 2014) privacy expectations around sensitive information on MTurk (Martin & Nissenbaum, 2017). For marketing, MTurk captures consumers most likely to be online (Tucker, 2014b) and is found to be a reliable source of respondents (Daly & Nataraajan, 2015).

[6] Respondent fatigue was checked by controlling for later vignettes in the respondents' sequence (the sequence number of the vignette was captured and ranged from 1 to 40). Additional analysis is in Appendix B.

Table 4
Sample descriptive characteristics.

	Survey 1	Survey 2	Survey 3
Vignette Factors:	Privacy factors	Trust factors	Trust & privacy
N (Users)	250	99	403
N (Vignettes)	10,000	3960	16,120
DV	− 13.77	− 6.46	− 13.49
SD	26.39	13.56	22.96
ICC Null	21.4%	5.2%	16.9%
R2	0.746	0.758	0.760

$$Y_i = \beta_i + \Sigma\beta_k V_k + e_i$$

4. Results

4.1. Impact of privacy violations on trust

According to Hypothesis 1, the presence of a violation of privacy expectations will decrease the user's trust in a website, all else being equal. To identify major violations of privacy expectations, an initial survey was run with privacy factors in the vignettes and the respondents rated the degree the vignettes met their privacy expectations. The results are in Table A3 in the Appendix and illustrate two practices as particularly important to violating privacy expectations: the secondary use of selling to a data aggregator and using the data to retarget friends.

Survey 1 captures whether the privacy violations – operationalized as the secondary use of selling to a data aggregator and using the data to retarget friends from Survey 0 – are considered trust violations (Survey 1). To test Hypothesis 1, the trust rating task was regressed on vignette and respondent controls for Survey 1. The results in Table 5 shows that some privacy violations – such as the secondary use of information – are judged to be more of a trust violation than a privacy violation such as the relative importance of selling information to a data aggregator ($\beta = -33.20$; $p < 0.00$) and using information to target friends ($\beta = -28.29$; $p < 0.00$).

To test if the importance of privacy violations remain important when traditional trust factors – ability, benevolence, and integrity – are taken into consideration, multilevel regression results of Survey 3 with trust factors and privacy factors is compared to Survey 1 with only privacy factors in Table 5. Adding the trust factors (ABI) diminishes but does not remove the role of privacy factors such as the secondary use of information and the type of information collected. For example, the importance of using information to target friends on trust decreases ($\beta_1 = -28.29$ v. $\beta_3 = -11.88$) as well as selling to a data aggregator ($\beta_1 = -33.20$ v. $\beta_3 = -14.28$).

4.2. Impact of privacy violations on importance of firm trustworthiness

Hypothesis 2 seeks to identify how firms violating privacy expectations could impact not only consumers' trust in the firm but also moderate the importance of ability and integrity on trust. To test the possible moderating impact of meeting or violating privacy expectations –operationalized as the secondary use of information based on Survey 0 – on trust factors, the interaction of each secondary use and trust factor (ability and integrity) was tested.

The results illustrate that Friend2ndUse moderates the importance of integrity to trust in a firm. When firms use information to target friends, the respondent, on average, decreases the relative importance of integrity (Friend2ndUse ∗ Integrity = − 3.12, $p < 0.00$) as shown in Fig. 3. The results were confirmed using a Chow test (Chow, 1960), where the sample was split into a condition with using the information to target friends (Friend2ndUse) and without using data for retargeting friends and the coefficients of each subsample's regression is

Table 5
Multi level regression results for surveys 1–3.

		Survey 1		Survey 2		Survey 3	
	Vignette factors:	Privacy factors		ABI		ABI and privacy	
		β	*p*	*β*	*p*	*β*	*p*
Trust factors	Ability			13.44***	0.00	6.06***	0.00
	Benevolence			4.85***	0.00	2.50***	0.00
	Integrity			28.96***	0.00	14.41***	0.00
	(*continuous*: 1–5)						
Context	BankingCxt	0.33	0.78	− 3.01	0.07	1.38	0.16
	PhotoCxt	− 2.08	0.08	2.13	0.19	0.10	0.92
	TravelCxt	− 0.04	0.98	− 0.09	0.96	0.38	0.70
	(*null = SearchCxt*)						
Info type	LocationInfo	− 7.26***	0.00			− 4.25***	0.00
	HistoryInfo	− 19.90***	0.00			− 11.39***	0.00
	VolunteerInfo	14.49***	0.00			10.66***	0.00
	(*null = DemoInfo*)						
Primary use	AdUse	− 4.83***	0.00			− 4.23***	0.00
	DiscountUse	1.51	0.20			0.04	0.97
	ImproveUse	2.95**	0.01			0.84	0.39
	(*null = tailor service*)						
Secondary use	Friend2ndUse	− 28.29***	0.00			− 11.88***	0.00
	Sell2ndUse	− 33.20***	0.00			− 14.28***	0.00
	Null2ndUse	22.20***	0.00			7.53***	0.00
	Internal2ndUse	28.44***	0.00			12.08***	0.00
	(*null = research 2nd use*)						
	StorageMths	− 6.34***	0.00			− 3.86***	0.00
	(*continuous*: 1–5)						
	Respondent controls						
	Age	− 1.13	0.43	− 3.27**	0.01	− 2.36*	0.02
	Gender	0.85	0.79	− 6.05*	0.03	− 0.65	0.78
	KnowInternet	0.94	0.62	− 0.48	0.72	1.54	0.20
	PurchaseOnline	3.29	0.27	− 0.60	0.84	1.15	0.51
	PrivacyConcern	− 0.11*	0.02	0.01	0.89	− 0.10***	0.00
	TrustSites	0.16***	0.00	0.06	0.07	0.14***	0.00
	CodingExp	− 0.80	0.59	1.81	0.17	− 0.68	0.49
	PrivacyImport	− 0.17**	0.01	− 0.03	0.65	− 0.09	0.05
	TrustDisposition	0.08**	0.01	0.06*	0.04	0.03	0.19
	Survey statistics						
	N (Users)	250		99		403	
	N (Vignettes)	10,000		3960		16,120	

* $p < 0.05$
** $p < 0.01$
*** $p < 0.001$

statistically compared. The coefficient for integrity decreases from 15.20 to 12.16 when the website retargets friends with the information ($\chi^2 = 17.91$, $p = 0.00$). Friend2ndUse has no moderating impact on ability ($p = 0.41$). Similarly, the interaction of Sell2ndUse * Ability is significant ($\beta = -1.69$ $p = 0.01$), yet selling to a data aggregator (Sell2ndUse) has no impact on the importance of integrity ($p = 0.771$). Finally, the interaction between Internal2ndUse and integrity is significant and positive ($\beta = +2.05$, $p = 0.00$) showing that firms who use the information for internal improvement are rewarded with greater weight on their integrity as compared to those using the data for research, selling to a data aggregator, or targeting friends.

The results show that firms are penalized twice with violations of privacy expectations. Violations around using information to target friends negatively impacts trust directly and diminishes the weight of a firm's integrity in trust judgments; selling to a data aggregator both negatively impacts trust directly and decreases the weight of ability on trust in a firm. On the other hand, using information to continuously improve the site positively impacts trust directly and positively impacts the importance of integrity on trust. Taken together, these results suggest a reinforcing effect of violations of privacy expectations on trust by impacting trust directly and having a reinforcing impact on trust factors such as integrity and ability.

4.3. How consumers differ in the importance of privacy for trust

Hypotheses 3 and 4 suggest respondents with a greater privacy despair as well as greater technological experience or online knowledge will place greater emphasis on privacy violations in forming trust judgments. Based on exploratory factor analysis explained in Section 3.3, the respondents were assigned two scores to capture both trust/privacy attitude (PrivacyDespair) as well as their knowledge and experience with relevant technology (TechSavvy). PrivacyDespair respondents have high valuation of and concern for privacy with lower trust in websites and trust dispositions: such respondents care about privacy but do not trust websites generally. The factor PrivacyDespair has a significant, direct, negative impact on the dependent variable (trust in this firm) of $\beta = -9.55$ ($p < 0.00$) for each quartile, yet does not have a moderating impact on the importance of privacy factors as hypothesized (see Fig. 2).

The respondent's TechSavvy score – a combination of knowledge of the Internet and coding experience – does not impact on the rating task directly. However, TechSavvy score does impact the relative importance of the privacy and trust factors as hypothesized. The interaction of TechSavvy and the privacy violating factors was included in a linear regression of the rating task on vignette factors. The results show that respondents with a higher TechSavvy score focus more on privacy violating factors such as the secondary use of information

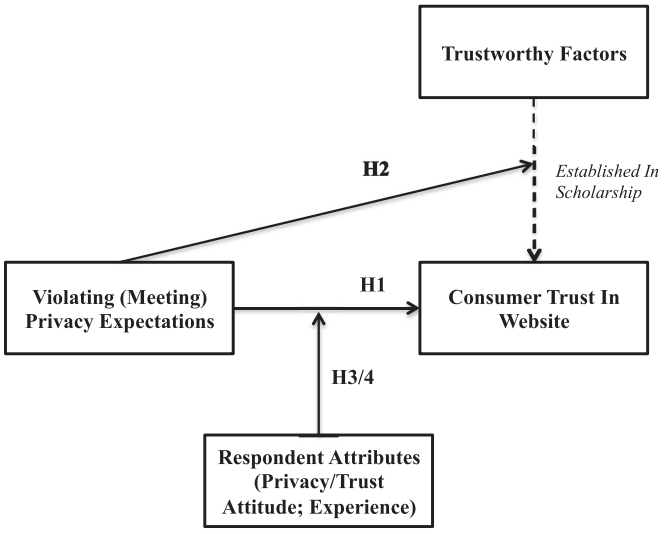

Fig. 2. Hypotheses.

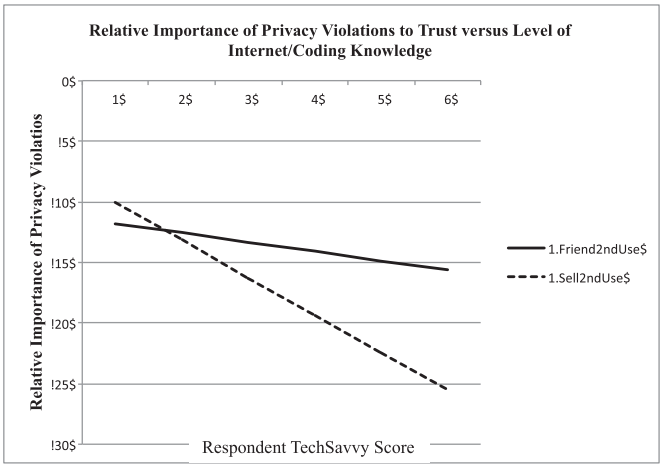

Fig. 3. Relative importance of privacy violations by TechSavvy score.

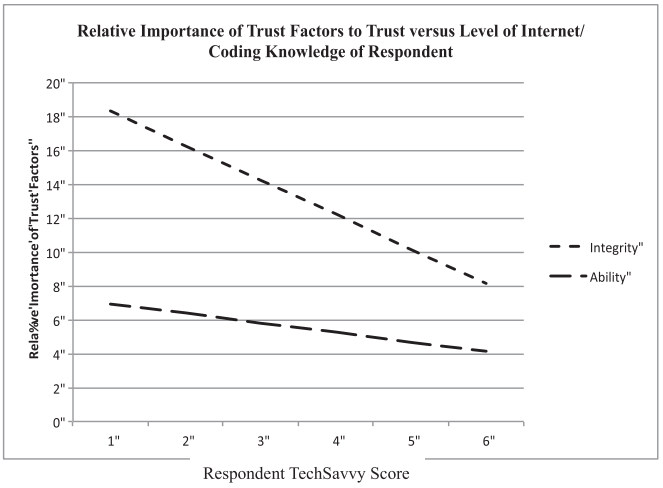

Fig. 4. Relative importance of trust factors ability and integrity on trust by TechSavvy score.

(TechSavvy ∗ Sell2ndUse = −2.09, $p = 0.01$) place less importance on the trust factors of ability (TechSavvy ∗ Ability = −0.56, $p = 0.02$) and integrity (TechSavvy ∗ Integrity = −1.93, $p < 0.00$) as shown in Figs. 3 and 4.

The results show PrivacyDespair scores impact the rating task directly whereas TechSavvy scores impact the relative importance of privacy and trust factors on user trust in a website. In other words, respondents with high and low TechSavvy scores have different privacy equations.

5. Implications and conclusion

5.1. Theoretical implications

5.1.1. Privacy and trust

The results support a reinforcing relationship between violations of privacy expectations and trust in a website online and fits within existing literature on the relationship between privacy and trust. Current scholarship shows that trust assuages privacy concerns by taking away the risk of information misuse (Bleier & Eisenbeiss, 2015; Rohm & Milne, 2004a; Xu et al., 2005) thus illustrating the importance of establishing trust to maintain consumer relationships online. This study focused on the importance of respecting privacy expectations to maintain trust. Previous work has shown general privacy concerns moderates trust in a firm (McCole, Ramsey, & Williams, 2010b) these results here reinforce these findings to illustrate the role of specific violations of privacy expectations on both trust and trust factors (see Table 6).

Interestingly, the two violations of privacy expectations used here – selling to a data aggregator and using data to retarget friends – diminished the impact of the ability and integrity of the focal firm respectively. This suggests different types of violations of privacy expectations may be perceived as different types of trust violations. Using the parlance of Pirson et al. (Pirson, Martin, & Parmar, 2015), retargeting friends was a matter of character whereas selling to a data aggregator was a matter of competence. Research suggests that breaches of agreements – even informal agreements – are a matter of breaking a promise and could, therefore, leave a user less impressed with other integrity signals of the firm in influencing trust. Further, ability if seen as mismanagement and competence, is a matter of both technological and managerial competence (Pirson et al., 2014) and the mismanagement of information could similarly leave users less focused on other ability signals. The type of trust violation could impact the type of rebuilding needed for trust violations.

However, the study examined how consumers trust a firm without an established relationship which is akin to the work on initial trust formation (McKnight, Cummings, & Chervany, 1998). Without an established relationship, consumers must rely on their tendency to trust as well as early trust signals from the firm. The respondents' reliance on a general disposition – such as the privacy despair control here – is supported by work on trust formation where trustors rely more on trusting tendencies than the trustworthiness of the trustee in initial trust formation (Pirson, Martin, & Parmar, 2016). Online, meeting or violation privacy expectations may be an important early signal of trustworthiness.

5.1.2. Consumer behavior

The study has implications for theories about consumer behavior online including social exchange theory (Schumann, von Wangenheim, & Groene, 2014) and consumer reactance (White, Zahay, Thorbjørnsen, & Shavitt, 2008). Within social exchange theory, a narrow exchange approach such as reciprocity, i.e. within the immediate transaction between the consumer and firm, may be limited since the problematic practices identified herein were well outside any immediate transaction. The violation of privacy expectations which decreased trust in the firm provided no immediate benefit to the consumer. In keeping with recent scholarship in social exchange theory (Martin & Murphy, 2016; Schumann et al., 2014), the argument may need to be less narrow and utilitarian and shift to a more normative

Table 6
Hypotheses and results.

Hypotheses	Results
H_1: The presence of a violation of privacy expectations will decrease the user's trust in a website, all else being equal.	Supported. The results show that privacy violations – such as the secondary use of information – are judged to be a trust violation.
H_2: The presence of a violation of privacy expectations will decrease the importance of trust factors on user's trust in a website.	Supported. The results show that firms are penalized twice with violations of privacy expectations. Violations around using information to target friends negatively impacts trust directly and diminishes the weight of a firm's integrity in trust judgments; selling to a data aggregator both negatively impacts trust directly and decreases the weight of ability on trust in a firm. On the other hand, using information to continuously improve the site positively impacts trust directly and positively impacts the importance of integrity on trust.
H_3: Consumers who have a greater concern about and valuation of privacy place greater emphasis on privacy violations in forming trust judgments.	Partially supported. The factor PrivacyDespair has a significant, direct, negative impact on the dependent variable (trust in this firm), yet does not have a moderating impact on the importance of privacy factors as hypothesized.
H_4: Consumers with greater technological experience or online knowledge will place a greater weight on privacy violations in making trust judgments.	Partially supported. The respondent's TechSavvy score – a combination of knowledge of the Internet and coding experience – does not impact on the rating task directly. However, TechSavvy score does impact the relative importance of the privacy and trust factors as hypothesized

reciprocity argument to be effective. Future work on social exchange theory and privacy may need to expand to a more generalized exchange where mutual trust promotes greater participation in generalized exchange systems (Takahashi, 2000; Yamagishi & Cook, 1993). A shift to a more generalized exchange to promote sharing and use of consumer information to support the advertising system would require a focus on institutional trust online since consumers currently lack trust in online advertising firms (Raine, 2016).

In addition, the judgments of individuals that appear contrary to reciprocity approaches may be due to consumer reactance as the psychological resistance of tracked information when freedom is perceived to be threatened (White et al., 2008). As shown by White et al. (2008), consumer reactance is greater when perceived utility is low – as was found in these results about selling data to a data aggregator. While White et al.'s focus was on personalization as seen in ads, the same consumer behavioral response could explain the findings here with the tracking of data as described in the vignettes. Work in surveillance suggests that individuals perceive harm due to the pervasiveness of data tracking regardless of how the data is actually used (Cohen, 2008). In other worlds, consumers' resistance to their freedom being threatened (White et al., 2008) would be found due to the mere pervasive tracking of information regardless if used in an ad. Consumer reactance could explain consumer behavior online and why more experienced consumers – who are aware of the tracking in order to react accordingly – use ad blockers (Rainie et al., 2013).

5.1.3. Categorizing consumers

The results have implications to how scholars and practitioners categorize consumers when attempting to understand privacy expectations. While consumers with greater privacy despair were found to be less trustful of websites overall, consumers with greater technology savvy were found to place greater importance on privacy factors than non-technology savvy. Westin's categorization or privacy concern respondent measurements used in academia are found to have limited utility in explaining consumers' behavior and reactions to online tracking and context-specific practices (Martin & Nissenbaum, 2017). These findings here with the 'privacy despair' type of consumer reinforces work identifying consumers with high valuation of privacy as well as low trust rather than a general privacy concern (Turow, Hennessy, & Draper, 2015b).

5.1.4. Privacy research

Privacy scholarship is continually in search of meaningful outcomes such as respondent's judgment that an act meets privacy expectations, a respondent's intent to purchase, a consumer's willingness to disclose or actual purchase in behavioral privacy, or individuals' click-through rate. Yet increasingly marketing practices rely on data which did not require knowing disclosure or consent thereby making a willingness to disclose or consumer choice less applicable (Martin & Murphy, 2016). However, reactance and trust remain important measures once the data collection practice is known. For research, these practices introduce the problem of hidden behavior that is difficult to capture with consumer behavior surveys – consumers are not aware of the tracking and sharing of consumer data online when online (Tucker, 2012). This experimental survey addresses the issue of respondents not being aware of actual practices. As consumers become more aware of the use of data aggregators (Federal Trade Commission, 2014; Pew Research Center, 2014; White House, 2014), consumer trust and normative judgments – such as reactance – as to the data practices of a website will become increasingly important. The results here suggest the potential to measure the resultant trust in a website or firm as an important outcome when examining privacy.

5.2. Limitations and future research

These findings should be viewed within the limitations of the factorial vignette survey. The factorial vignette methodology offers hypothetical scenarios and provides a bridge between experiments and carries the strengths and weaknesses of both types of empirical work. The methodology captures the complexities of real decision-making, and respondents are less susceptible to social desirability bias as in conventional surveys (Taylor, 2006; Wallander, 2009). However, the researcher bias can influence the inclusion of factors, and missing factors could change the final models. Further, 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.

5.3. Managerial implications

While Westin's categorizations of consumers as to their privacy concerns – e.g., privacy unconcerned versus privacy pragmatists – continue to be referenced and criticized in practice (Hoofnagle & Urban, 2014; Westin, 2001), this study found alternative categorization around consumers' privacy despair and tech savvy. Consumer experience as important is in keeping with finding 'insiders' to a community as understanding privacy norms better than outsiders (K. E. Martin, 2012; Pew Research Center, 2014): technological experience and online knowledge may constitute 'insider' status for data privacy norms online. Firms would need to understand their consumers' privacy norms and expectations as well as the variance of experience before setting data practices.

In addition, this study did not offer consumers the ability to control their experience online, since the vignettes were presented to the respondent to be judged as-is. However, consumer control has been found to be important to assuaging privacy concerns; respondents were less concerned when given more options in their privacy notice even when the actual data practices remained consistent (Tucker, 2014a). In effect, these findings present a worst-case scenario of consumers being allocated no control or options online. According to Tucker's findings (Tucker, 2014a), consumer control may be a vehicle to assuage perceived violations.

While regulatory agencies, such as the FTC, continue to focus on adequate notice and choice, this study has shown that specifics about data practices matter to consumers rather than mere adequate notification. As data practices become more widely known through researchers and investigatory journalism, consumers are able to make trust judgments regardless of the substance of the privacy notice. This paper suggests that firms violating user privacy are penalized twice: first in the users' trust in the firm and also in the users' importance given to the firm's trust factors of ability or integrity. These results suggest that privacy violations may be particularly difficult to recover from without the benefit of perceived ability or integrity. On the other hand, a potential competitive advantage may be realized with respecting privacy with increased trust and the greater importance given to the firm's ability and integrity. In this study, firms that utilized information to improve their service rather than target friends or sell to a data aggregator not only were trusted more but their integrity also counted more for future trust judgments. The study's results are in keeping with approaches to privacy as a form of strategy (Martin, Borah, & Palmatier, 2016) and illustrate how privacy could be a critical piece of building trust online and as a basis of a competitive advantage – particularly when the negative impact of privacy violations on trust is realized by a competitor.

Appendix A

Table A1
Control variables.

Question	Label	Values
Gender	Male	1
	Female	2
Age	Under 18	1
	18–24	2
	25–34	3
	35–44	4
	45–54	5
	55–64	6
	65 +	7
40 Vignettes	*I trust this website.*	− 100… + 100
Knowledge internet	I don't know any technical details	1
How would you judge your knowledge of the technical aspects that make the Internet work?	I have a vague idea of the technical details	2
	I have a good idea of the technical details	3
	I am very knowledgeable	4
	I am an expert	5
Privacy concern	*I am concerned that online companies are collecting too much personal information about me.*	− 100… + 100
Trust in websites	*In general, I trust websites.*	− 100… + 100
Coding experience	I have coded in too many languages to count	1
How many programming languages have you used for coding?	I have coded in several (2–4) programming languages	2
	I have coded in one programming language	3
	I have coded but do not remember the language	4
	None - I have never coded	5
Privacy important	*In general, I believe privacy is important*	− 100… + 100

Table A2
Sample descriptive characteristics.

	Survey 0	Survey 1	Survey 2	Survey 3
Vignette factors:	Privacy factors	Privacy factors	Trust factors	Trust & privacy
DV:	Expect DV	Trust DV	Trust DV	Trust DV
N (Users)	93	250	99	403
N (Vignettes)	3720	10,000	3960	16,120
DV	− 15.98	− 13.77	− 6.46	− 13.49
SD	30.80	26.39	13.56	22.96

ICC Null	26.6%	21.4%	5.2%	16.9%
R2	0.719	0.746	0.758	0.760

Control variables	Mean	S.d.	Mean	S.d.	Mean	S.d.	Mean	S.d.
KnowInternet	2.98	1.03	2.84	0.92	2.90	1.04	2.90	0.98
PurchaseOnline	2.34	0.56	2.26	0.54	2.27	0.45	2.34	0.62
PrivacyImportant	55.63	40.58	56.67	40.55	53.23	47.07	53.36	40.26
TrustSites	− 17.12	47.56	− 5.56	44.94	4.67	44.03	− 9.29	46.69
CodingExp	2.13	1.26	1.98	1.15	2.00	1.10	1.95	1.22
PrivacyImportant	79.47	25.77	80.02	27.47	78.87	28.61	79.33	24.32
TrustDisposition	8.76	54.28	20.26	49.85	18.33	49.03	21.10	52.03
Gender	1.41	0.49	1.40	0.49	1.39	0.49	1.44	0.50
Age	3.12	0.89	3.22	1.10	3.28	1.00	3.36	1.08

Table A3

	Survey 0		Survey 1	
Vignette factors:	Privacy factors		Privacy factors	
DV:	Privacy expect DV		Trust DV	
	β	*p*	*β*	*p*
BankingCxt	− 0.235	0.91	0.328	0.78
PhotoCxt	− 0.501	0.81	− 2.079	0.08
TravelCxt	3.121	0.13	− 0.035	0.98
(null = SearchCxt)				
LocationInfo	− 12.516	0.00	− 7.255	0.00
HistoryInfo	− 21.908	0.00	− 19.903	0.00
VolunteerInfo	17.976	0.00	14.486	0.00
(null = DemoInfo)				
AdUse	− 2.072	0.31	− 4.826	0.00
DiscountUse	0.481	0.81	1.514	0.20
ImproveUse	2.291	0.26	2.950	0.01
(null = Tailor service)				
Friend2ndUse	− 22.246	0.00	− 28.287	0.00
Sell2ndUse	− 28.692	0.00	− 33.195	0.00
Null2ndUse	22.568	0.00	22.200	0.00
Internal2ndUse	20.798	0.00	28.439	0.00
(null = Research 2nd use)				
StorageMths	− 6.551	0.00	− 6.338	0.00
Respondent controls				
Age	− 3.818	0.21	− 1.134	0.43
Gender	0.864	0.88	0.851	0.79
KnowInternet	3.227	0.38	0.942	0.62
PurchaseOnline	2.318	0.67	3.288	0.27
PrivacyConcern	− 0.221	0.01	− 0.110	0.02
TrustSites	0.231	0.00	0.155	0.00
CodingExp	− 3.796	0.15	− 0.802	0.59
PrivacyImport	− 0.053	0.70	− 0.167	0.01
TrustDisposition	0.021	0.72	0.081	0.01
Survey statistics				
DV	− 15.98		− 13.77	
SD	30.80		26.39	
ICC Null	26.6%		21.4%	
R2	0.719		0.746	
N (Users)	93		250	
N (Vignettes)	3720		10,000	

Appendix B. Respondent fatigue

As to respondent fatigue, additional analysis is included below. After the results testing respondent fatigue, possible explanations are included in this response.

First, a dummy 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 -0.04, $p = 0.96$. The Last 5 vignettes received a lower rating task on average for tracking vignettes only (Last5Qs beta $= -2.34$, $p = 0.05$). There was no significant impact for the dummy variable the First20Q or Last20Q. The mean for each grouping are in Table B1 where the consistency across the vignettes is illustrated.

Table B1
Differences and similarities in beginning and ending vignettes.

	First 20	Last 20	First 35	Last 35
Mean	− 13.15	− 13.53	− 13.25	− 13.46
SD	56.66	54.95	55.91	55.43
N	8060	8060	14,105	14,105

Second, the survey sample was split in two ways for a regression analysis. First, the samples were split between the first 20 vignettes and second 20 vignettes to see if the relative importance of vignette factors differed. This was then repeated for subsamples with and without the first and last 5 vignettes to capture a possible learning curve (over the first 5) and fatigue (over the last five vignettes). The coefficients for each regression analysis are in Fig. B1 for the primary trust factors and secondary use factors used as privacy violations in the analysis. The relative importance (the coefficients) are consistent across the samples. The differences across subsamples are insignificant and the theoretical findings as to the relative importance of contextual and individual factors to privacy expectations remain the same.

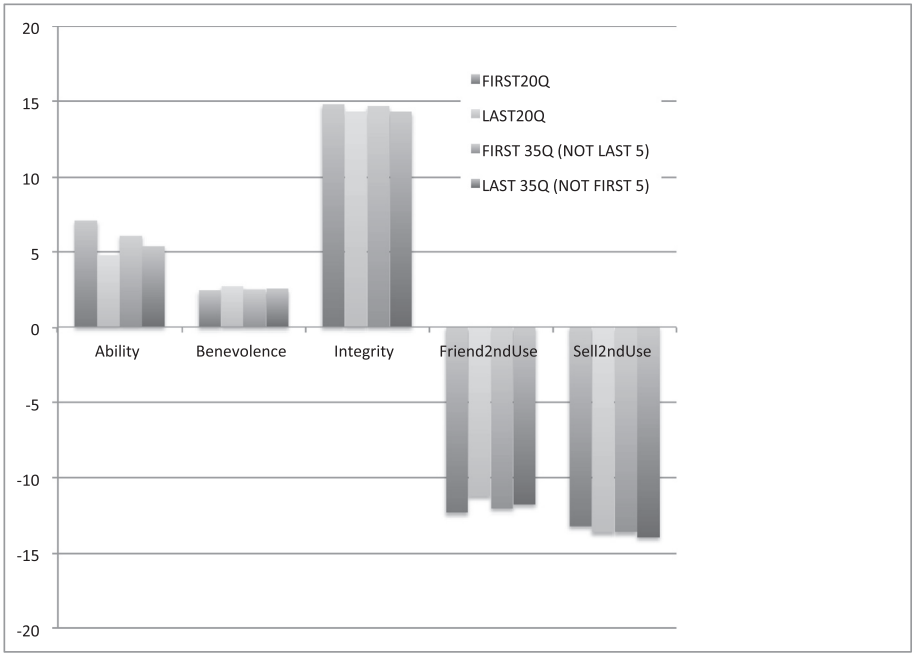

Fig. B1. Comparison of Coefficients of Each Subsample Run in Table B1.

There are a few possible reasons why fatigue would not be a problem in this design. First, the number of sentences read is actually akin to most surveys. For example, including standard controls, 1–2 survey instruments which include 10–20 + questions each, additional closing survey questions, and attention checks, a standard research survey could require 50 + different sentences to carefully read answer. Here, the vignettes are kept fairly simple by design in that the vignettes are standard in their format and the type of rating task asked. This is another reason why the methodology is insistent on one rating task for all the vignettes – answering different types of questions is tiring as they have different error terms.

Appendix C. Factor analysis

Factor	Eigenvalue	Difference	Proportion	Cumulative
Factor1	1.43111	0.44723	0.5926	0.5926
Factor3	0.4547	0.2676	0.1883	1.1883
Factor4	0.1871	0.12104	0.0775	1.2658
Factor5	0.06607	0.09284	0.0274	1.2931
Factor6	− 0.02677	0.08839	− 0.0111	1.282

Factor7	− 0.11517	0.03615	− 0.0477	1.2343
Factor8	− 0.15132	0.02937	− 0.0627	1.1717
Factor9	− 0.18069	0.05325	− 0.0748	1.0969
Factor10	− 0.23394	.	− 0.0969	1

Variable	Factor1	Factor2	Uniqueness
Age	0.0546	− 0.1808	0.9643
KnowInternet	0.1406	0.6297	0.5837
PurchaseOnline	− 0.0393	0.0487	0.9961
PrivacyConcern	0.6528	− 0.1166	0.5603
TrustSites	− 0.7669	0.0587	0.4084
CodingExp	0.0819	0.5668	0.672
PrivacyImportant	0.4341	− 0.1046	0.8006
TrustDisposition	− 0.4393	− 0.0336	0.8059
_eq2_R2	0.0047	− 0.0949	0.991

Variable	Factor1	Factor2	Uniqueness
Age			0.9643
KnowInternet		0.643	0.5837
PurchaseOnline			0.9961
PrivacyConcern	0.6626		0.5603
TrustSites	− 0.7677		0.4084
CodingExp		0.5727	0.672
PrivacyImportant	0.4444		0.8006
TrustDisposition	− 0.4305		0.8059
_eq2_R2			0.991

References

Anton, A., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security and Privacy, 8*(1), 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. Retrieved from https://books.google.com/books?id=bG1eBAAAQBAJ.

Awad, N. F., & Ragowsky, A. (2008). Establishing trust in electronic commerce through online word of mouth: An examination across genders. *Journal of Management Information Systems, 24*(4), 101–121.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*(4), 133–152.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3), 245–270.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*(1), 211–241.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing, 91*(3), 390–409.

Cases, A.-S., Fournier, C., Dubois, P.-L., & Tanner, J. F. (2010). Web site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. *Journal of Business Research, 63*(9), 993–999.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2–3), 181–202.

Chow, G. (1960). Tests of equality between sets of coefficients in two linear regressions. *Econometrica, 28*(3), 591–605. http://dx.doi.org/10.2307/1910133.

Cohen, J. E. (2008). Privacy, visibility, transparency, and exposure. *The University of Chicago Law Review* (pp. 181–201). .

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* (pp. 47–70). .

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115. http://dx.doi.org/10.1287/orsc.10.1.104.

Daly, T. M., & Nataraajan, R. (2015). Swapping bricks for clicks: Crowdsourcing longitudinal data on Amazon Turk. *Journal of Business Research, 68*(12), 2603–2609.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 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*(8), 877–886.

Elsbach, K., & Currall, S. (2012). Understanding threats to leader trustworthiness: Why it's better to be called “incompetent” than “immoral”. In R. Kramer, & T. Pittinsky (Eds.). *Restoring trust in organizations and leaders* (pp. 217–240). Oxford University Press.

Everard, A., & Galletta, D. F. (2005). How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems, 22*(3), 56–95.

Federal Trade Commission (2014). *Data Brokers: A call for transparency and accountability.* FTC. Retrieved from http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *SIGMIS Database, 33*(3), 38–53.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems, 24*(4), 275–286.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

Gefen, D., & Pavlou, P. A. (2012). The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research, 23*(3-part-2), 940–959. http://dx.doi.org/10.1287/isre.1110.0395.

Goldstein, D. G., Suri, S., McAfee, R. P., Ekstrand-Abueg, M., & Diaz, F. (2014). The economic and cognitive costs of annoying display advertisements. *Journal of Marketing Research, 51*(6), 742–752.

Hainmuellera, J., Hangartnerb, D., & Yamamotod, T. (2015). Validating vignette and conjoint survey experiments against real-world behavior. *PNAS, 112*(8), 2395–2400.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999a). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999b). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *The Information Society, 15*(2), 129–139.

Hoffmann, C. P., Lutz, C., & Meckel, M. (2014). Digital natives or digital immigrants? The impact of user characteristics on online trust. *Journal of Management Information Systems, 31*(3), 138–171.

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest L. Rev. 49. Wake Forest L. Rev* (pp. 261–). .

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems, 48*(2), 407–418.

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research, 34*(3), 334–423.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858–873.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human Computer Interaction, 25*(1), 1–24.

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*(6), 607–635.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: The effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of Applied Psychology, 89*(1), 104.
Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75–91.
Lim, K. H., Sia, C. L., Lee, M. K., & Benbasat, I. (2006). Do I trust you online, and if so, will I buy? An empirical study of two trust-building strategies. *Journal of Management Information Systems, 23*(2), 233–266.
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*(4), 336–355.
Martin, K. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday, 18*(12).
Martin, K. (2015). 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*(2), 210–227. http://dx.doi.org/10.1509/jppm.14.139.
Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569. http://dx.doi.org/10.1007/s10551-015-2565-9.
Martin, K., & Nissenbaum, H. (2017). Measuring privacy: Using context to expose confounding variables. *Columbia science and technology law review*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709584.
Martin, K., & Shilton, K. (2015). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*.
Martin, K. D., Borah, A., & Palmatier, R. W. (2016). Data privacy: Effects on customer and firm performance. *Journal of Marketing*. http://dx.doi.org/10.1509/jm.15.0497.
Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science,* 1–21.
Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 111*(4), 519–539. http://dx.doi.org/10.1007/s10551-012-1215-8.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995a). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995b). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. http://dx.doi.org/10.5465/AMR.1995.9508080335.
McCole, P., Ramsey, E., & Williams, J. (2010a). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9), 1018–1024.
McCole, P., Ramsey, E., & Williams, J. (2010b). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research, 63*(9), 1018–1024.
McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. http://dx.doi.org/10.1287/isre.13.3.334.81.
McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 473–490.
Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4), 00.
Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research*.
Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing, 21*(1), 5–15.
Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing. *European Journal of Marketing, 41*(9/10), 1173–1202.
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*(4), 32–48.
Pan, L.-Y., & Chiou, J.-S. (2011). How much can you trust online information? Cues for perceived trustworthiness of consumer-generated online information. *Journal of Interactive Marketing, 25*(2), 67–74.
Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331–338.
Pavlou, P. A., & Dimoka, A. (2006). The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation. *Information Systems Research, 17*(4), 392–414.
Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*(1), 37–59. http://dx.doi.org/10.1287/isre.1040.0015.
Pew Research Center (2014). Public perceptions of privacy and security in the post-Snowden era. Retrieved from http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.
Pirson, M., Martin, K., & Parmar, B. (2014). Public trust in business and its determinants. In J. D. Harris, B. Moriarty, & A. C. Wicks (Eds.). *Public trust in business* (pp. 116–152). Cambridge University Press.
Pirson, M., Martin, K., & Parmar, B. (2015). Formation of stakeholder Trust in Business and the role of personal values. *Journal of Business Ethics,* 1–20. http://dx.doi.org/10.1007/s10551-015-2839-2.
Pirson, M., Martin, K., & Parmar, B. (2016). Public trust in business and its determinants. *Business & Society,* 1–35. http://dx.doi.org/10.1177/0007650316647950.
Poppo, L., & Zenger, T. (2002). Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal, 23*(8), 707–725.
Raine, L. (2016). The state of privacy in post-Snowden America. *Pew research center*. Retrieved from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). *Anonymity, privacy, and security online.* (Pew Research Center).
Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets, 24*(2), 135–149.
Rohm, A. J., & Milne, G. R. (2004a). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research, 57*(9), 1000–1011.
Rohm, A. J., & Milne, G. R. (2004b). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research, 57*(9), 1000–1011. http://dx.doi.org/10.1016/S0148-2963(02)00345-4.
Rossi, P. H., & Nock, S. L. (1982). *Measuring social judgments: The factorial survey approach.* Beverly Hills: Sage Publications.
Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing, 19*(4), 305–335.
Sauer, C., Auspurg, K., Hinz, T., & Liebig, S. (2011). *The application of factorial surveys in general population samples: The effects of respondent age and education on response times and response consistency. Vol. 5*, 89–102 (Presented at the Survey Research Methods).
Schofield, C. B. P., & Joinson, A. N. (2008). *2 Privacy, trust, and disclosure online*.
Schumann, J. H., von Wangenheim, F., & Groene, N. (2014). Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*(1), 59–75.
Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems, 11*(3), 325–344.
Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62–73.
Smith, D., Menon, S., & Sivakumar, K. (2005). Online peer and editorial recommendations, trust, and choice in virtual markets. *Journal of Interactive Marketing, 19*(3), 15–37.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly,* 167–196.
Takahashi, N. (2000). The emergence of generalized exchange. *American Journal of Sociology,* 1105–1134.
Taylor, B. J. (2006). Factorial surveys: Using vignettes to study professional judgement. *British Journal of Social Work, 36*(7), 1187–1207.
Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems, 16*(2), 214–232.
Tucker, C. E. (2012). The economics of advertising and privacy. *International Journal of Industrial Organization, 30*(3), 326–329.
Tucker, C. E. (2014a). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562.
Tucker, C. E. (2014b). The reach and persuasiveness of viral video ads. *Marketing Science, 34*(2), 281–296.
Turow, J., Hennessy, M., & Draper, N. (2015a). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
Turow, J., Hennessy, M., & Draper, N. (2015b). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.* Annenburg School of Communication1–24. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). *Americans reject tailored advertising and three activities that enable it.* (Available at SSRN 1478214).
Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online trust: State of the art, new frontiers, and research potential. *Journal of Interactive Marketing, 23*(2), 179–190.
Wallander, L. (2009). 25 Years of factorial surveys in sociology: A review. *Social Science Research, 38*(3), 505–520.
Westin, A. F. (2001, May 8). *Opinion surveys: What consumers have to say about information privacy.* (Prepared Witness Testimony, The House Committee on Energy and Commerce, W. J. "Billy" Tauzin, Chairman).
White House (2014). Big data: Seizing opportunities, preserving values. Retrieved from http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters, 19*(1), 39–50.
Xu, H., Wang, H., & Teo, H. H. (2005). Predicting the usage of P2P sharing software: The role of trust and perceived risk. *Proceedings of the 38th Hawaii International Conference on System Sciences*.
Yamagishi, T., & Cook, K. S. (1993). Generalized exchange and social dilemmas. *Social Psychology Quarterly,* 235–248.
Yang, S., & Lynn, M. (2014). More evidence challenging the robustness and usefulness of the attraction effect. *Journal of Marketing Research, 51*(4), 508–513.

Kirsten Martin is an associate professor of Strategic Management and Public Policy at the George Washington University's School of Business. She has been funded by the National Science Foundation to study online privacy. Dr. Martin is a member of the advisory board for the *Future Privacy Forum* and the Census Bureau's National Advisory Committee for her work on privacy and the ethics of Big Data. Dr. Martin is a fellow at the *Business Roundtable Institute for Corporate Ethics* for her work on stakeholder theory and trust. She earned her B.S. Engineering from the University of Michigan and her MBA and Ph.D from the University of Virginia's Darden Graduate School of Business. Her research interests center on online privacy, technology, corporate responsibility, and stakeholder theory.