J Bus Ethics
DOI 10.1007/s10551-012-1215-8

Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract

Kirsten E. Martin

Received: 21 December 2010 / Accepted: 13 January 2012

Abstract A growing body of theory has focused on privacy as being contextually defined, where individuals have highly particularized judgments about the appropriateness of what, why, how, and to whom information flows within a specific context. Such a social contract understanding of privacy could produce more practical guidance for organizations and managers who have employees, users, and future customers all with possibly different conceptions of privacy across contexts. However, this theoretical suggestion, while intuitively appealing, has not been empirically examined. This study validates a social contract approach to privacy by examining whether and how privacy norms vary across communities and contractors. The findings from this theoretical examination support the use of contractual business ethics to understand privacy in research and in practice. As predicted, insiders to a community had significantly different understandings of privacy norms as compared to outsiders. In addition, all respondents held different privacy norms across hypothetical contexts, thereby suggesting privacy norms are contextually understood within a particular community of individuals. The findings support two conclusions. First, individuals hold *different* privacy norms without necessarily having *diminished* expectations of privacy. Individuals differed on the factors they considered important in calculating privacy expectations, yet all groups had robust privacy expectations across contexts. Second, outsiders have difficulty in understanding the privacy norms of a particular community. For managers and scholars, this renders privacy expectations more difficult to identify at a distance or in deductive research. The findings speak directly to the needs of organizations to manage a diverse set of privacy issues across stakeholder groups.

Keywords Privacy · Social contract theory · Contractual business ethics · Factorial vignette methodology · Survey

Introduction

Privacy is a subject of substantial interest to management scholars and practitioners. One need not look far to find organizations grappling with the privacy expectations of potential customers, employees, or end users. And scholarship has recognized the role of privacy in such stakeholder relationships: privacy is integral to organizational trust (Pavlau et al. 2007) and fairness (Culnan and Armstrong 1999) and can be a strategic advantage (Smith 2004; Culnan and Armstrong 1999). As such, privacy is a pervasive management issue that crosses management disciplines in addition to business ethics including corporate governance (Beales and Muris 2008; Milberg et al. 2000), strategy (Culnan and Armstrong 1999), and information technology (Smith et al. 1996; Son and Kim 2008; Straub and Collins 1990).

While all agree that privacy is important, disagreement exists on what privacy means and what it encompasses (Charters 2002; Van de Hoven 2008). Definitions of privacy vary—from private information being that which is inaccessible (Warren and Brandeis 1890; Elgesem 1999; Persson and Hansson 2003), controlled (Westin 1967; Alder et al. 2007), or fairly gathered (Bennett 1992; Ashworth and Free 2006; Peslak 2005)—and the concept remains "fuzzy" (Van de Hoven 2008). This is problematic in that performing research on the strength of privacy

K. E. Martin (✉)
The Catholic University of America, 309 McMahon Hall, 620 Michigan Ave NE, Washington, DC 20064, USA
e-mail: martink@cua.edu

Published online: 31 March 2012

norms becomes an exercise in testing the presence of an analyst's conception of privacy in a given population, for a given stakeholder, or within a given issue. For example, actions, such as background checks or Internet monitoring, are positioned as violations of privacy because the actions are not in conformance with an analyst's definition of privacy (Alder et al. 2007). Similarly, individual's who do not agree with the analyst's definition of privacy are presumed to not find privacy important (e.g., Acquisti and Gross 2006) or unethical (Winter et al. 2004).

A growing body of theoretical scholarship has focused on privacy as being contextually defined, thereby defining and examining privacy norms within relationship, situation, or context (Brenkert 1981; Nissenbaum 2004; Solove 2006; Moor 1997; Jiang et al. 2002). Contextual approaches view privacy expectations as the negotiated information norms within a particular community or situation. Individuals are privacy pragmatists (Beales and Muris 2008) who exchange information for specific benefits, i.e., better relationships, power, team cohesion, etc., and these exchanges carry forth actual and hypothetical social contracts (Culnan and Bies 2003). A contextual approach to privacy may explain why management research and practice struggle to identify a universally accepted, static definition of privacy.

In addition, such a contextually defined understanding of privacy could produce more practical guidance for managers and organizations who face a range of privacy issues across stakeholders. Organizations and managers have employees, users, and future customers all with possibly different conceptions of privacy across contexts: employee monitoring (Smith and Tabak 2009; Persson and Hansson 2003; Martin and Freeman 2003; Miller and Weckert 2000), behavioral marketing (Charters 2002), online commerce (Pollach 2005; Shaw 2003; Awad and Krishman 2006), RFID technology (Peslak 2005), data storage (Culnan and Williams 2009), and social networking (Martin 2010)—to name only a few—each contain their own contextual influences on privacy expectations. Tactics in managing employee information may not translate to the expectations of potential customers, and static approaches to privacy do not guide managers across relationships, situations, or contexts.

This article validates a social contract approach to privacy through an experimental empirical study. As explained more fully below, a social contract approach to privacy extends current work within context-dependent approaches and allows individuals within a particular community to develop local privacy norms about what, why, how, and to whom information flows, while respecting universal social contract principles such as consent, voice, and exit among others (Donaldson and Dunfee 1994; van Oosterhout et al. 2006).

A social contract approach to privacy is supported theoretically (Culnan and Armstrong 1999), and would be particularly well suited to the stakeholders and issues of organizations and managers. However, little empirical work has been done to test a social contract approach to privacy as social contract approaches, in general, remain empirically challenged (Dunfee 2006; Glac and Kim 2009; van Oosterhout et al. 2006; Soule 2002): allowing for locally defined norms renders contextual approaches to privacy difficult to test empirically.

Factorial vignette survey methodology is used to examine the possibility of locally negotiated authentic privacy norms within particular communities (Rossi and Nock 1982; Jasso 1990). Rather than test for the presence of a static definition of privacy, the factorial vignette method supports identifying the privacy factors and their relative importance—the privacy norms—that respondents take into consideration in making a judgment about privacy within particular communities (Jasso 2006; Wallander 2009). This study is a theoretical examination, and the findings will support or not support the use of social contract approaches to explain privacy norms. Such research seeks the generalizability of ideas rather than the generalizability of data patterns within a specific population (Lynch 1982).

This study builds on and contributes to both privacy literature and contractual business ethics (CBE) scholarship. First, I extend existing literature on contextual approaches to privacy that suggest privacy norms are dependent upon particular relationships and context. Finding empirical evidence of a social contract approach to privacy would suggest that rather than developing a singular litmus test for privacy, practitioners, and scholars would focus on identifying relevant contracting communities and the factors and their relative importance those individual take into consideration in their privacy expectations.[1]

In addition, social contract approaches comprise an important movement in business ethics and management with both theoretically robust hypothetical narratives and

[1] For example, Smith et al's (1996) *concern for information privacy* (CFIP) survey instrument is used as a measure of an individual's concern for privacy in general and within particular contexts, the authors note, "As privacy increases in importance, it behooves [us] to consider the complexity of individual's concerns, the factors that may cause increased levels of concerns, and the outcomes of those concerns" (1996, p. 191). While the latter two ideas have been empirically investigated, we have yet to tackle unpacking the factors that individuals' take into consideration in forming expectations of privacy for specific situations. As Smith et al. note, CFIP is not only applicable to particular contexts and situations but also should be "used in interpretive research on *what the meaning of information privacy is* for individuals …apart from and prior to whether a positivist theory would define it to be" (1996 emphasis added).

critiques within CBE generally as well as the highly cited integrative social contract theory (ISCT) (Donaldson and Dunfee 1994; Heugens et al. 2006; Dunfee 2006; Phillips and Johnson-Cramer 2006; Husted 1999). The identification of the relevant community and local authentic norms is "partially if not entirely" an empirical task (Husted 1999). Yet, local authentic norms have proven difficult to empirically examine (Glac and Kim 2009). The quasi-experimental methodology employed here allows for the inductive generation of implicit privacy norms agreed upon within a contract community through statistical analysis. This research not only builds on CBE but also contributes to CBE by meeting the call to for more task-directedness and domain-specificity in social contract empirical work to focus on a precise issue the contract is supposed to fulfill (Wempe 2005).

Theoretical Foundation and Hypotheses Development

A social contract approach to privacy is an outgrowth of current contextual approaches to defining privacy in philosophy. *Relationship-based* privacy scholars justify or define privacy based on inter-personal relationships and view privacy as an agreement between individuals (Brenkert 1981). Privacy has long been seen as necessary for social exchanges: discriminately sharing information allows us to form different relationships with different people (Fried 1984; Rachels 1975) and is useful to converse and trade (Singleton 1998). *Situation-based* scholars, on the other hand, allow for privacy rules to be context dependent regardless of the individuals involved (Jiang et al. 2002; Solove 2006). Combining the two approaches, Moor (1997) views privacy as attached to a situation or zone where different people may be given different levels of access for different kinds of information at different times (Moor 1997), thus making privacy simultaneously more realistic yet more difficult to empirically examine or to develop specific guidance for managers.

However, the most thoroughly *context-dependent* approach to privacy is perhaps Nissenbaum's *privacy as contextual integrity* (2004, 2009). Nissenbaum views privacy as the negotiated agreements about how information is accessed and distributed. Maintaining privacy norms entails the "information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it" (Nissenbaum 2004, p. 101). In doing so, Nissenbaum ties privacy expectations to norms within specific contexts and incorporates both the relationship and the situation in defining privacy.

Nissenbaum suggests privacy norms are based on our expectations governing a particular piece of information being passed between particular individuals within a context. For example, for a medical professional, information such as medical history and overall medical concerns are expected to be transmitted to the doctor and her staff. However, in a different context, such as the workplace, the same information would be considered inappropriate for the individuals in that space. Even a question about medical history is deemed inappropriate and a violation of privacy expectations when at work. Within a context, for every given set of individuals and information, there exists an expectation about how information will flow and whether or not the information is expected, appropriate, or inappropriate.

Key to Nissenbaum's privacy as contextual integrity is how the main components work together—individuals, information, and how information flows—within a particular context. Privacy norms vary based on specific relationships and situations; individuals decide not only the type of information that is allowable, expected, or demanded, but also where, why, and how the information is to be used. Shopping online, talking in the break room, and divulging information to a doctor are governed by the information norms of that particular social context. Contextual approaches that take into consideration the relationships and situation in the definition of privacy are particularly attractive to organizations and management scholars given the range of stakeholder concerns which change on a regular basis.

Nissenbaum and other contextual approaches are a seismic shift to approaching privacy given the predominance of static, universally applied definitions of privacy in the access-view and control-view of privacy (Nissenbaum 2009; Schoeman 1984; Johnson 2004). Where the access-view of privacy would have privacy norms defined as a function of the accessibility of information (privacy norms $= f$(access, information)), and the control-view of privacy would have privacy norms defined as a function of the degree of control of the information (=f(control, information), context-dependent approaches assume privacy norms are a function of the individuals, information, and context (=f(information, individuals, *context*)). In other words, "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). Individuals do not hold universally applicable, substantive definitions of privacy; rather individuals disclose information within a particular context with an understanding of the privacy rules that govern that context.

By allowing for context-dependent privacy norms, Nissenbaum's theory of privacy is consistent with a social contract approach to privacy. First, similar to social contract approaches, such as integrated social contract theory (Donaldson and Dunfee 1994) or CBE more generally (van

Oosterhout et al. 2006), context-dependent definitions of privacy are positioned as an alternative to universally defined norms. Rather than privacy expectations being set by a context-independent definition, such as when privacy is defined as the degree of access to or control over information, Nissenbaum's theory suggests that the definition of privacy—whether information is expected, appropriate, or inappropriate to be shared—are developed, negotiated, and understood based on the context. Access may be important in a particular context but immaterial in another. In other words, *individuals have highly particularized judgments about the appropriateness of what, why, how, and to whom information flows.* Similarly, CBE has been found to be particularly well suited for managers and organizations by addressing ethical issues which vary based on communities rather than universally applicable norms (van Oosterhout et al. 2006; Spicer et al. 2004).

Second, Nissenbaum's use of context is closely related to the use of community within a social contract approach. Context is defined as "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)" (Nissenbaum 2009, p. 132) and shares facets of ISCT's communities, which are self-circumscribed group of people with shared tasks, values, goals, who are capable of establishing norms (Donaldson and Dunfee 1994; Glac and Kim 2009). Important to both theories, individuals are given the space to develop norms that fit the particular requirements of their community or context given the shared goals, norms, and values. This moral free space within the contract community corresponds to the context in Nissenbaum's privacy as contextual integrity.

These contexts and communities are particular. Both theories place the focus on identifying relevant communities and their local norms, and both approaches attempt to move from the abstract to the highly particularized. In fact, social contract theory has been termed a theory in search of an application (Heugens et al. 2006) with future research to be both task and domain specific (Wempe 2005). Using a social contract approach to privacy meets the need for CBE to have informing applications and empirical enrichment (Heugens et al. 2006) and addresses the identified problem that social contract approaches in business ethics are at too high a level (Thompson and Hart 2006).

Finally, social contract approaches extend Nissenbaum's insightful theory. A social contract approach to privacy addresses some of the concerns of relativism endemic to context-specific definitions of privacy while supporting the contextually defined privacy norms and expectations, which are the strength of Nissenbaum's privacy as contextual integrity (2004). As noted by Nissenbaum, a concern of context-specific definitions of privacy is the lack of moral authority associated with norms developed internal to a given group or context (2004, p. 125). Without a universally recognized definition of privacy, privacy rules could be considered completely relative to the situation, where privacy is defined as what people in a particular society and at a particular time are prepared to disclose (Miller and Weckert 2000). A social contract approach adds structural and procedural norms to provide a mechanism to evaluate local norms.[2]

Empirical Examination of Social Contract Approach

A social contract approach to privacy is not only supported by context-dependent definitions of privacy in theory but also offers a research platform to study context-dependent privacy norms. Social contract approaches include multiple levels of contracting rules (Donaldson and Dunfee 1999): authentic norms negotiated within the contracting space, which are fluid and continually up for negotiation (Phillips and Johnson-Cramer 2006), and universal, second-order contract norms that transcend contract spaces (van Oosterhout et al. 2006). The variance in local norms across communities renders social contract approaches theoretically interesting yet empirically difficult. The empirical examination of a social contract approach to ethical issues

[2] A social contract approach to privacy offers three theoretical additions to analyze local privacy norms. First, locally negotiated, implicit social contracts are always beholden to structural, procedural, and (for some) substantive universal principles (van Oosterhout et al. 2006) to remain legitimate. Social contract approaches are multilevel, contextually rich frameworks allowing for specific contractors within a contracting community the moral free space to develop authentic and legitimate norms of behavior (Donaldson and Dunfee 1994). However, these local norms must also abide by the more universal and thin second order norms such as the rights of consent, voice, and exit (Donaldson and Dunfee 1994; Dunfee 2006; Heugens et al. 2006). As such, contracting has an internal morality without the need for external substantive guidance (van Oosterhout et al. 2006).

In addition, these locally negotiated privacy norms can be analyzed through both actual and hypothetical social contracts to address "norms of decency, etiquette, sociability, convention, and morality" (Nissenbaum 2004; see also, Tavani 2008). While privacy as contextual integrity focuses on the actual negotiated privacy norms, social contract approach would add a possible additional layer of analysis in the form of the *hypothetical* social contract which would have moral weight. We could ask, what norms would reasonable individuals agree to given minimal social contract standards of consent, voice, and exit? Finally, social contract theory would suggest the prescriptive value in protecting the integrity *of the boundaries* of the contracting community and their moral free space and not only the norms within the space. In other words, viewing these negotiated privacy norms as a social contract highlights the moral importance in protecting the bounds of the context in Nissenbaum's privacy as contextual integrity. If outsiders were to dictate the privacy norms of a group of co-workers or between a husband and wife, their rights of negotiating privacy norms would be violated. In fact, such a privacy intrusion or violation is referred to as *decisional privacy* (Allen 1999) or passive privacy (Floridi 2006).

consists of identifying both *convergent* norms that are possible candidates for substantive second-order norms, as well as *divergent* norms that are possible candidates for local, authentic norms.

Examining divergence across contexts and contractors has taken different forms in empirical work on social contract theory within management and business ethics scholarship. First, analyzing differences in norms *across contracting communities*, as in the difference between business norms in Russia and the US (Spicer et al. 2004), validates a social contract approach by identifying local norms within previously defined communities. Studies compare responses in one community to responses in a different community to identify whether and how norms diverge. Alternatively, identifying the difference in norms *across contractors* also validates a social contract approach to ethical issues (e.g., Bailey and Spicer 2007). Insiders to a community are theorized to understand local, authentic norms better than outsiders and comparing insiders to outsiders' judgments about a particular community examines a social contract approach to a particular ethical issue.

Importantly for a social contract perspective, insiders have a different perspective on the local norms of the particular community and not in general. The first two measurements of divergence—across communities and across contractors—narrow in on how to empirically validate a social contract approach to an ethical issue, while leaving open the possibility that insiders have a generally different approach to ethics or decision making that manifests in their judgment about a particular community under study. Yet, insider status should only impact local norms within contract community to validate a social contract approach. For example, in an examination of business norms within the sales, insiders with experience in sales have divergent norms from outsiders (Robertson and Ross 1995). The possibility remains that individuals with sales experience have a different understanding of business norms in general, including within sales.

Two options further isolate the role of insider status on understanding local norms to validate a social contract approach to an ethical issue. The first option is to study a range of contractors and non-contractors—as in the difference between norms of local Russians, Americans working in Russia, and Americans working in America (Bailey and Spicer 2007)—to examine how individuals might have learned local norms within a community. By comparing the responses of Americans working in America with Americans working in Russia, the analysis isolates the impact of contractor status from the impact of nationality. Similarly, isolating the impact of insider status from common demographic characteristics can also be achieved by controlling for gender, age, and student-status in any analysis. Both tactics attempt to parse out the impact of being a contractor from demographic attributes that may explain divergent norms and expectations.[3]

The second tactic involves ensuring insider status impacts only local norms using a control group. In order to isolate the effect of insider status on understanding the local norms, the divergence in norms in reference to a control community must also be included. For example, proximity to a particular community, such as doing business in Russia (Bailey and Spicer 2007) or sales (Robertson and Ross 1995), could cause a general shift in normative judgments and values rather than a specific learning of the norms of the particular community.

Hypothesis Development

Social contract research in management and business ethics outlines a methodology to study communities and local norms that can be leveraged to develop hypotheses about whether and how privacy norms vary based on context. The focus here is on the possibility of local authentic privacy norms based on a particular community. The definition of what is and is not a privacy norm is regularly assumed to be consistent across contexts and universally understood across individuals; in other words, the current default theoretically is the *convergence* of privacy norms across individuals and across communities. In fact, a social contract approach "cannot be used to select a single set of action guiding norms" (van Oosterhout et al. 2006, p. 534), but is best used to explore divergence in norms. Therefore, to explore if contractors have different negotiated authentic norms about privacy within specific contracting communities, divergence across communities and across individuals is theoretically interesting as the divergence of norms illustrates boundaries of social contract spaces or the difference between contractors and non-contractors (Bailey and Spicer 2007).

Individual-Level Drivers of Privacy Norms: Proximity to Contracting Community

Social contract theory is designed to be helpful with community-specific moral norms (Husted 1999), and first-level contracting norms are negotiated within the moral free space of a *specific* contracting community. Those within a contract community—contractors or insiders—

[3] This is not the case for *all* examinations of social contract approach to ethical issues. For example, the claim of Bailey and Spicer (2007) is that different nationalities and nations have different local norms. As a social contract approach is used to explore more targeted communities, as has been called for in literature (Heugens et al. 2006; Dunfee 2006), the need for a 'control' community may be more necessary to isolate the impact of insider status on the particular community's norms rather than a general change in disposition.

best understand the implicit understandings of local authentic norms (Donaldson and Dunfee 2002), where outsiders struggle to identify definitive norms (Dunfee 2006). Insiders differ from outsiders not due to their demographic information or their actual participation in negotiating social contract norms. Rather, insiders are knowledgeable (Strong and Ringer 2000) and are different from those "who have little knowledge of local practices" (Spicer et al. 2004, p. 611). Even actual contractors vary in their "deeper knowledge of cultural differences and stronger personal affiliations and commitments" to a given community (Bailey and Spicer 2007, p. 1467).

Insider status is but one mechanism to measure the degree of knowledge of local norms. Insiders are usually designated by their membership status within a community, yet knowledge rather than membership is the pertinent characteristic of these individuals. Previously, commitment, or the degree to which an individual is included in a particular community, has been used as a measurement of the strength of the attachment to the community and presumed to influence the strength of the effect of the local norms on ethical beliefs and behavior (Bailey and Spicer 2007). The key facet of interest is not the degree of commitment, which could be conflated with the strength of the community norms, but the individual's ability to understand the local norms (van Oosterhout et al. 2006).

Knowledge or understanding of local norms need not emanate from membership status in a particular community. For example, experience in a particular industry's sales organization would constitute closeness to a sales community under study, but those with general sales experience may also have a close affiliation and knowledge, and those in business may have a better understanding of the norms of a sales group than those who have never worked in an organization.

While individuals' range of knowledge and understanding of local norms has been operationalized as insiders and the degree of commitment, the pertinent characteristic of knowledge of local norms can be gained by *proximity* to the contracting community more generally. Proximity is the closeness of the individual to the norms, goals, and values based on experience or exposure. Those with insider status have more experience and knowledge, and constitute a theoretical extreme in a range of individuals with proximity. Similarly, those with a greater commitment through tenure or exposure would have close proximity in comparison to newcomers or outsiders. Insiders and outsiders constitute one bifurcation of the range of proximity, but multiple points along a proximity continuum may be studied. For example, comparing individuals with sales experience to students without any experience offers two theoretically interesting groups with extreme variance in proximity. However, other groups with limited business experience or sales experience in a different industry could also constitute two points along the proximity continuum between the theoretical extremes.

Therefore, the first hypothesis tests the degree to which the understanding of local privacy norms diverge based on the individuals' proximity to a contracting community. The understanding of privacy norms should diverge between inside contractors and outsiders to the community if a social contract approach to privacy holds.

Hypothesis 1 Within a particular contracting community, insiders have different authentic norms about privacy—the factors and their relative importance—from outsiders to the contract community.

Community-Level Drivers of Privacy Norms: Contracting Scenarios

The second source of divergence is across communities. Social contract theory would suggest that both the situation and the actual contractors influence authentic norms (Donaldson and Dunfee 1999), and the contracting scenario provides a unique logical vantage point from which to view an ethical quandary such as privacy expectations. Contract communities are self-defined groups of individuals who interact in the context of shared tasks, values, or goals and are capable of negotiating norms behavior (Donaldson and Dunfee 1994). Social contracts depend on specific relationships within the contracting community, where some communities have stronger relationships with codified goals, boundaries, and norms that may even be institutionalized. Similarly, Nissenbaum notes, contexts vary in their articulation of characteristics such as norms, roles, activities, power structures, goals, and values. More defined communities would have more characteristics recognized explicitly or implicitly with a greater amount of institutionalization (Nissenbaum 2009). Such well-defined communities are similar to families, whereas less-defined communities are looser affiliations and may be closer to neighborhood groups (Bailey and Spicer 2007).

To ensure divergent local norms are not due to individual differences within the contractors, the degree to which privacy norms change due to the contracting community must also be tested. Therefore, not only do insiders have different authentic norms than outsiders based on the proximity to the contracting community but also individuals will have different authentic norms in a well-defined community as compared to a control group of individuals. In other words, for a social contract approach to privacy to hold, individuals should *not* have consistent privacy norms across contracting communities. Local norms should be specific to the particular contracting community.

Hypothesis 2a Individuals hold different authentic norms about privacy—the factors and their relative importance—within a particular contracting community as compared to a control contract community.

If the claim is that individuals develop different norms based on the specific contracting community, as is the case with social contract approach to privacy and Nissenbaum's privacy as contextual integrity, the individuals should *change* norms across contexts or communities. To ensure the impact of insider status is specific to the particular community, the role of insider status on the differential local norms can also be examined. Controlling for the ethical judgments of a generally understood control community allows the analysis to isolate the impact of insider status on the particular community apart from any impact on a general disposition. In other words, the *incremental* or *differential* privacy norms afforded to a well-defined community should differ based on proximity. Specifically in regards to privacy, Beales and Muris (2008) note that consumers within a specific information exchange are best positioned to identify any additional (or reduced) privacy expectations in that relationship.

Insiders should diverge in their understanding of local, authentic norms in comparison to outsiders relative to a control community. Here, the privacy norms of a well-defined team would be examined in comparison to the norms of a less-defined and commonly understood community. Any differential privacy expectations afforded to contractors within a well-defined contracting scenario is best understood by actual contractors. In other words, across contracting communities, insiders and outsiders should diverge on the *differential* privacy norms afforded to well-defined contracting communities above and beyond a control group.

Hypothesis 2b The differences between authentic privacy norms within a particular contracting community and less-defined contracting scenarios will be moderated by the individual's proximity to the contracting community.

Methods

This study examines the theoretical suggestion that individuals develop highly contextualized privacy norms within contract communities. This research is a theoretical examination, which seeks the generalizability of ideas rather than the generalizability of data patterns within a specific population (Lynch 1982). The findings from this experimental study will or will not support the use of CBE to understand privacy to research and practice (Levitt and List 2007, p. 153).

The objective of this study is to identify and compare individuals' privacy norms across contracting communities. Namely, what are the factors and their relative importance that contribute to an expectation that information should or should not be shared? Toward this end, the factorial vignette survey methodology was employed. The methodology was developed to investigate human judgments (Rossi and Nock 1982), and supports the theoretical investigation into if privacy norms can be explained using a social contract approach as developed in the hypotheses. In a factorial vignette survey, a set of vignettes is generated for each respondent, where the vignette factors or independent variables are controlled by the researcher and randomly selected, and respondents are asked to evaluate these hypothetical situations. Factorial survey methodology allows for the simultaneous experimental manipulation of a large number of factors through the use of a contextualized vignette (Ganong and Coleman 2006).[4]

While established within sociology (Rossi and Nock 1982; Jasso 2006; Wallander 2009), the factorial vignette survey technique is less established within business ethics or management.[5] The methodology has been used in sociology to study such issues as political action (Jasso and Opp 1997), conceptions of mental illness (Thurman, Lam, and Rossi 1988), and fairness of compensation (Jasso 2006). The factorial vignette approach allows the researcher to examine (a) the elements of information used to form judgments, (b) the weight of each of these factors, and (c) how different subgroups of the respondents agree on (a) and (b) (Nock and Gutterbock 2010). Factorial vignette methodology assumes "some level of agreement among people in a small group/community as to a combination of factors that is important to take into consideration when making a judgment" (Wallander 2009, p. 514), which renders the methodology particularly well suited to the examination of a social contract approach to privacy where norms should vary based on subgroups of the respondents. These factors and their associated coefficients are the *equations-inside-the-head* (Jasso 2006) of respondents and, herein, would constitute the negotiated authentic norms of privacy.

[4] In comparison, in experiments, factors are designed orthogonal to each other but manipulated one at a time; however, in a traditional survey, many factors are examined but are not necessarily orthogonal to each other (Appelbaum et al. 2006). Such an experimental design is useful for a "clean" test of theory (Levitt and List 2007).

[5] While the use of vignettes within surveys in business ethics is well established (Weber 1992), the factorial vignette survey methodology stems from sociology and is distinct in its methodology and analysis as explained below. See also Wallander (2009) for a review and Jasso (2006) for a technical article on the methodology; see Smith et al. (2007) for the single use of the methodology in business ethics.

Generalizability for theoretical research, as compared to effects application research, investigates relationships among ideas or constructs, and the researcher "seeks to understand those constructs that have influence on a variety of behaviors in a variety of situations." (Lynch 1982). As such, naturally occurring stimuli and responses are often ill-suited to testing hypotheses of interest to theoretical researchers leading such researchers into the laboratory "where manipulations and measures can be concocted that have relatively simple mappings onto the constructs of concern" (Lynch 1982, p. 233). In a similar argument by Strong and Ringer (2000), social contract research need not model reality precisely, but should be designed to test the principles of ISCT within a context.

Therefore, in order to examine a social contract approach to privacy based on the hypotheses developed, the study must include (a) community-level drivers (different contract communities), (b) individual-level drivers (insiders and outsiders), and (c) privacy factors impacting privacy expectations that may vary based on (a) and (b) to examine whether and how individuals have highly particularized judgments about the appropriateness of what, why, how, and to whom information flows.

Privacy Factors

The primary explanatory variables in this study are the privacy factors that constitute the vignettes. The number and levels of factors combine to create the universe of possible vignettes (Nock and Gutterbock 2010) and should be guided by theory, reasoning, and wisdom (Jasso 2006; Wallander 2009). 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. 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. The "Appendix" contains a table of factors as well as a sample vignette.

The privacy factors are based on Nissenbaum's privacy as contextual integrity (2004) as well as privacy theory to examine the hypotheses *around whether and how individuals have highly particularized judgments about the appropriateness of information flows around what, why (the community), where, how, and to whom*. The analysis centers on whether and how the importance or weight of these factors diverge across individuals and across communities rather than the weight of one particular factor as being generalizable to a larger population. The *importance* of what, where, how, and to whom information is shared should vary across communities and contractors.

What: Content

Rather than have general rules on privacy based solely on the physical location or the individuals in a relationship, Nissenbaum (2004) suggests that individuals construct different expectations based on the *type* or *attribute* of information rather than a label of public or private; what is considered personal or sensitive may vary based on the respondent and the context of the exchange (Nissenbaum 2009). Five levels of content were systematically varied in the vignettes from (1) information that is independently knowable by individuals outside community to simulate that which is usually deemed "public" (e.g., "Housing decisions for next semester"), information necessary for the community goals since privacy norms support the goals of the context (Nissenbaum 2009) (e.g., "Who is going to start for the next game/how the projects were assigned"), and information traditionally labeled sensitive or private such as family or medical information ("A date that went horribly wrong "or "Problems with his mom" or "An embarrassing medical condition"). A wide range of information allows respondents to identify highly particular privacy expectations about each piece of information and to inductive indentify through the analysis the importance of family or medical information relative to a known standard of easily accessible information ("housing decisions for next semester").

How: Access

Traditional approaches to privacy posit restricting access to information as foundational to protecting privacy (Martin 2010). Consistent across definitions and justifications of privacy is a minimal standard of privacy that allows individuals and their information to remain inaccessible (Moor 1997; Johnson 2001). Information that is not intentionally disclosed—as in overheard or coerced information—is regularly regarded as receiving greater privacy expectations based on both the control-view and the access-view of privacy. To test the impact of information that is willingly shared as compared to that which is coerced or overheard, vignettes varied on how the information was disclosed. Information was willingly shared, overheard, or reluctantly shared to capture a range of how information was disclosed.

Where: Location

Some attempts to parse privacy are based on the location, information form, or technology (Johnson 2004), others view location as a tertiary factor in our social norms about sharing information (Nissenbaum 2009). Nissenbaum's contextual theory of privacy does not emphasize

technology or location as an important factor in determining privacy expectations by context. Yet, as noted by Smith et al. (2011), a general assumption underlying information privacy scholarship is that new technology applications lead to different privacy norms and expectations. To allow for this theoretical ambiguity, physical location of the vignette scenario varied including a small, enclosed, role-based physical space such as a locker room and a large, easily accessible space such as a cafeteria. In addition, technological platforms—e-mail and Facebook—were included to identify if technology is a factor to privacy norms. The communication technologies parallel the physical locations of the information exchange in the vignettes.

To Whom: Distribution

According to Nissenbaum's theory of privacy, *who* receives the information is a factor in our privacy expectations. As noted by Nissenbaum, specific individuals are taken into consideration when assessing the privacy expectations of a context. Individuals may consider sharing information with other contractors to be expected, whereas sharing information outside the contract space may be considered wrong (Nissenbaum 2004; Jiang et al. 2002). Therefore, vignettes included scenarios where information was shared inside the community with peers and supervisors as well as with individuals outside the contracting community.

Social Contracting Factors

Contracting Communities

Within CBE, the contracting community is a self-defined, self-circumscribed group of people who interact in the context of shared tasks, values, or goals. They are capable of establishing norms of ethical behavior for themselves (Donaldson and Dunfee 1994). Communities may differ in the types of forces they exert on individuals. For example, families exert more pressures for inclusion than neighborhood organizations (Bailey and Spicer 2007). In order to identify changes in privacy expectations across contracting communities, the vignette scenarios were set in either a well-defined, norm-generating community (a varsity collegiate athletic team) or an less-defined group (a randomly assigned student group). Athletic teams have been compared to business teams previously (Katz and Koenig 2001): they are similar in structure and motivation and, importantly for this study, membership and stability are important. Athletic teams are well-defined, goal-oriented, norm-generating communities of individuals who have the opportunity and need to develop authentic norms; these groups fit the definition of contracting communities from Donaldson and Dunfee (1994).

Membership

Social contract approaches place an emphasis on contractors understanding authentic local norms before being held accountable for them (Donaldson and Dunfee 1999). Therefore, new members of a team may be held to a different standard compared to more senior members who are fully knowledgeable of the authentic norms of the community.

Insiders and Outsiders

In order to identify subgroups who understand and identify with the given contracting community, respondents were asked the level of membership on an athletic team and their associated hours per week with the team. As has been noted, individuals have different levels of experience and exposure in communities, which influences the strength of the community effects on ethical beliefs and behavior (Bailey and Spicer 2007). The respondent's proximity to the contracting community (varsity athletic teams) delineated insiders versus outsiders to the contract space in the analysis below and represent end points of a range of proximity to the contracting community. Additional control variables included sex, degree earned, years post-college, and undergraduate status allow for a more granular parsing of proximity to the contracting community—male varsity athletic team.

The Vignettes

The vignettes were constructed by varying several factors along dimensions or levels. A deck of vignettes for each respondent was randomly created with replacement as the respondent was taking the survey from a vignette universe of 1,200 possible factor combinations ($1{,}200 = 2(\text{community}) \times 3(\text{access}) \times 5(\text{content}) \times 4(\text{distribution}) \times 2(\text{new member})$). For factorial vignette surveys, the number of vignettes is typically set at 10–60 vignettes for each respondent to answer. However, the survey was designed to give participants the option to opt out of the survey at 10, 20, and 40 vignettes in an attempt to mitigate the recurring issue of respondent fatigue or respondent burden (Nock and Gutterbock 2010), i.e., when the judgments *and associated errors* cannot be assumed to be independent due to correlation within a single respondents' answers, whereas typically vignettes are pooled as is independent. For each rated vignette, the associated rating, factor levels, and the vignette script was preserved as well as the vignette sequence

number.[6] See "Appendix" for sample vignettes as well as the factors.

Sample

The sample was recruited via e-mail within a single institution using a snowball technique: heads of departments and teams were the primary contacts who forwarded the survey to their members. Both students and non-students were recruited to represent a range of proximity to the contracting space described in the vignette. Of the 831 respondents, undergraduate students comprised only 50.6% of the sample.

Dependent Variable: Privacy Expectation

Respondents were asked to judge the named protagonist in the story who shared information with others. After each vignette, the same question was asked the respondent "Should [NAME] have shared the information with others?" with the computer program inserting the randomly chosen male name which matched that chosen for the associated vignette. The rating task remained consistent throughout the survey as per factorial vignette survey methodology. The rating task was an ordinal scale, with the dependent variable ranging from 0 (Expected to Share information) to 4 (Wrong to Share Information) (Nissenbaum 2004).

Analysis

The data in this study was in two levels: the vignette level factors and the respondent level control variables. For this survey, 831 respondents rated a range of 0–40 vignettes resulting in 21,187 rated vignettes or observations. If N is the number of the respondents with Level 2 demographic variables and K is the number of vignettes answered with Level 1 factor variables, the general equation is:

$$\ln(P(Y \leq j)) = \ln(Y_j) = \alpha_j + \beta X \quad (1)$$

$$Y_{nk} = \beta_0 + \Sigma\beta_j V_{jk} + \Sigma\gamma_h R_{hn} + u_n + e_k \quad (2)$$

where Y_{nk} is the rating of vignette k by respondent n, V_{jk} is the jth factor of vignette k, R_{hn} is the hth characteristic of respondent n, β_0 is a constant term, β_j and γ_h are regression coefficients, u_n is a respondent-level residual (random effect), and e_{ik} is a vignette-level residual. The model conceptualizes the ratings as a function of the factors of the situation described in the vignette and the characteristics of the respondent. Therefore, the analysis below focuses on these factors and their relative importance, which constitute the privacy norms for that individuals, and not the mean privacy expectation or the ordinal rating that the information should or should not be shared.

In testing the hypotheses, ordinal regression was used to identify the factors that influence the privacy expectations of respondents. Ordinal regression compares the odds of an event occurring compared to the odds of that event not occurring, rather than absolute changes in the dependent variable itself as in traditional Ordinary Least Squares (OLS) regression models.[7] Strong associations between explanatory variables and ratings are represented by coefficients farther away from 0.0 and odds ratios (ORs) farther away from 1.0 (since OR = exp(β)). A negative (positive) coefficient would have an OR less (greater) than one and would signify the associated explanatory variable would have a upward (downward) impact on the rating task.

Results

To explore the current null hypothesis–that respondents hold a static and universal definition of privacy—a general model was developed by regressing the rating task against all vignette level variables. This model assumed all respondents will have similar models for privacy, yet this general equation did not pass any goodness of fit statistics.[8]

The data was divided into vignettes based on contracting communities. This permitted the identification of important factors within a particular well-defined community (varsity athletic team scenarios) and within a less-defined contracting community (the assigned student team) as per factorial vignette survey methodology (Wallander 2009). For hypothesis testing, insiders and outsiders to the contracting community were identified by running several ordinal regressions based on demographic variables. The

[6] Respondent fatigue was a factor for some respondent groups. I created two dummy variables to signify vignette ratings with a sequence number over 30 and over 20. If the ordinal regression model demonstrated a significant impact on the rating task by either dummy variable, those associated vignette ratings were discarded for that model. The regression was rerun without the offending data. However, a larger design issue came from the respondents' *learning curve*—presumably from the novelty of the survey design. Once the first two vignette ratings for each respondent (sequence numbers 1 and 2) were discarded for all respondents, the model fit criteria and parallel lines assumptions improved dramatically. I discarded all vignette ratings with a sequence number of 1 or 2 for the entire analysis.

[7] For ordinal variables, the outcome is *at or below given outcome* Y_j. Ordinal dependent variables—such as the traditional Likert scale rating task used here—do not necessarily meet the assumptions required of traditional OLS models (O'Connell 2006; Kennedy 2003) which impacts analysis below.

[8] Statistically significant ORs are assessed by testing the significance of the regression coefficient using a Wald test. In addition, the fit of the model was determined using the goodness-of-fit statistics and the test of parallel lines.

Table 1 Comparison of mean privacy expectations across proximity to contracting community and across contracting scenarios

Group	Well-Defined community				Less-Defined community				Less-Defined vs. Well-Defined	
	n	Mean priv exp	M–W *Z* stat[a]	Sig	*n*	Mean priv exp	M–W *Z* stat[b]	Sig	M–W *Z* stat[c]	Sig
Insider	389	2.84	n/a		397	3.03	n/a		(2.310)	0.02
Outsider 1	479	2.98	(2.238)	0.03	428	3.00	(0.056)	0.96	(0.216)	0.83
Outsider 2	707	3.02	(2.412)	0.02	626	3.13	(1.372)	0.17	(2.240)	0.03
Outsider 3	1074	3.16	(4.831)	0.00	996	3.28	(3.932)	0.00	(2.799)	0.01

[a] Comparison of group mean to insiders within a well-defined community using Mann–Whitney

[b] Comparison of group mean to insiders within a random team using Mann–Whitney

[c] Comparison of well-defined to random team within group using Mann–Whitney

degree subgroups agree or disagree on those factors was assessed using goodness-of-fit measures of the regression equations. Four groups proved to be theoretically and statistically different in their assessments of privacy: male varsity athletes with high hours per week (Insiders), female varsity athletes with high hours per week (Outsiders 1), male respondents who never played a sport (Outsiders 2), and female respondents who never played a sport (Outsiders 3).[9] Table 1 reports the sample size of each contracting group as well as the mean privacy expectations for each contracting scenario. Each group rated information as more likely to be "Ok to Share" in the well-defined team and more likely to be "Wrong to Share" in the less-defined team. However, as is analyzed below, the factors each take into consideration when making that determination varied across individuals and across scenarios.

Table 2 shows the effects of the vignette factors as independent variables on the dependent variable with both significant standard βs and ORs provided to illustrate the relative importance of the vignette factors on the rating task. For example, while the categories of dating, family, and medical information are consistently associated with higher categories on the privacy rating, the amount of influence varies based on both the contracting group and the contracting community. The use of ORs permits the comparison of factors and their importance across models: we can say, all things being equal, vignettes with medical content *raise the odds* of finding information Wrong to Share by 8.8 times for the third outsider group in Model 4b as compared to vignettes without medical information.

Hypothesis 1 predicts that within a defined contracting scenario, such as the varsity athletic team vignettes, inside contractors will have a different understanding of the authentic privacy norms from individuals outside the contract community. To test the first hypothesis, I performed ordinal regression analysis for each of the contracting groups as depicted in Table 2. Models 1a–4a demonstrate that within well-defined contracting scenarios, these different respondent groups did not agree on either the expectations of privacy (dependent variable) or the privacy norms (factors and relative importance). Perhaps most strikingly, insiders did not take into consideration how the information is accessed—if it was coerced or overheard—in their expectations of privacy. In other words, coerced and overheard information is treated the same as that which is willingly shared. In comparison, three outsider groups placed considerable emphasis on coerced and overheard information as both factors have positive coefficients with coerced information raising the odds of finding the information Wrong to Share by 1.9–4.5 times. All other factors held constant, the third outsider group—female respondents who never played a sport—were 4.5 times as likely to find coerced information more Wrong to Share compared to lower rating categories, whereas insiders—who matched the demographics of the vignette scenario and would be considered actual contractors in this contracting space—do not take access into consideration *at all* when assessing privacy expectations inside the well-defined scenario. Figure 1 depicts the different priority given to coerced information for the different groups: the further the group was away from the contracting community, the more the norms of coerced information diverged from authentic norms of community insiders.

Similarly, the type of content plays a different role in assessing privacy expectations based on the individual's proximity to the contract community as shown in Table 2. For those closest to the contracting space, dating information was not a factor in assessing a privacy violation and was treated the same role-based information, whereas outsiders were between 2.3 and 3.3 times as likely to find the information Wrong to Share if the information was about dating. In other words, the content matters more to

[9] Other combinations were examined including those who ever played a sport, those who played IM or varsity, and those who played varsity athletics but with only 10–20 h/week. In addition, initial analysis did not differentiate based on sex. However, goodness-of-fit metrics did not indicate the models illustrated any agreement among these alternative respondent groups.

Table 2 Ordinal regression models organized by vignette scenarios

Independent variables	Well-Defined community (athletic team scenarios)								Less-Defined community (random team scenarios)							
	Insiders		Outsider 1		Outsider 2		Outsider 3		Insiders		Outsider 1		Outsider 2		Outsider 3	
	Model 1a		Model 2a		Model 3a		Model 4a		Model 1b		Model 2b		Model 3b		Model 4b	
Factors	β	OR	β	OR	β	OR	β	OR	β	OR	β	OR	β	OR	β	OR
Access																
Coerced info	0.000	1.0	1.206	3.3	0.631	1.9	1.499	4.5	0.000	1.0	0.000	1.0	0.751	2.1	0.000	1.0
Overheard info							0.581	1.8								
Willingly shared																
Content																
Role based													(0.669)	0.5		
Personal	0.000	1.0	0.000	1.0	1.210	3.4	0.864	2.4	1.707	5.5	1.153	3.2	1.297	3.7	1.801	6.1
Family	0.823	2.3	1.424	4.2	1.500	4.5	1.896	6.7	1.986	7.3	1.259	3.5	1.612	5.0	1.916	6.8
Private	1.621	5.1	1.528	4.6	2.415	11.2	1.991	7.3	1.940	7.0	1.758	5.8	1.580	4.9	2.174	8.8
Public																
Location																
Verbal outside			0.651	1.9												
e-mail																
FB feed	(0.833)	0.4			(0.699)	0.5	(0.598)	0.5					(0.831)	0.4		
FB post	(1.463)	0.2			(1.221)	0.3	(0.606)	0.5			(1.251)	0.3	(0.718)	0.5	(0.754)	0.5
Verbal inside																
Distribution																
To leaders																
To captains											0.705	2.0			0.474	1.6
Outside group																
Inside group																
UG status			(0.569)	0.6	(0.789)	0.5	0.152	1.2	(0.888)	0.4	(0.857)	0.4	(0.645)	0.5		
All coefficients listed with significance <0.001																
Model fit																
2LL intercept only $\chi 2$	90.724		99.369		257.310		345.924		77.555		65.869		163.392		197.845	
Sig	0		0		0		0		0		0		0		0	
Pseudo R^2																
Cox and Snell	0.208		0.187		0.305		0.275		0.217		0.143		0.230		0.180	
Nagelkerke	0.224		0.201		0.334		0.304		0.237		0.154		0.252		0.203	
McFadden	0.088		0.078		0.148		0.137		0.008		0.059		0.108		0.090	
Pearson	0.014		0.057		0.000		0.009		0.369		0.026		0.015		0.031	
Deviance	0.269		0.055		0.128		0.037		0.399		0.252		0.374		0.072	
Parallel lines assumption																
Sig	0.479		0.111		1.000		0.001		0.187		0.023		0.000		0.150	

those well outside the contracting community when assessing expectations within the contracting space than those actually within the contract community. The findings support the prediction in Hypothesis 1 that actual contractors will have different authentic norms about privacy from individuals outside the contract community. Further, those farthest outside the contract community diverged the most from the authentic privacy norms of the community as defined by insiders to that space as illustrated in Fig. 1.

Hypothesis 2a predicts individuals hold different authentic privacy norms across contracting scenarios. To test the second hypothesis, I calculated the relative change in coefficients between well-defined contract scenarios and less-defined team scenarios ($\Delta\beta = \beta_a - \beta_b$) in Table 3.

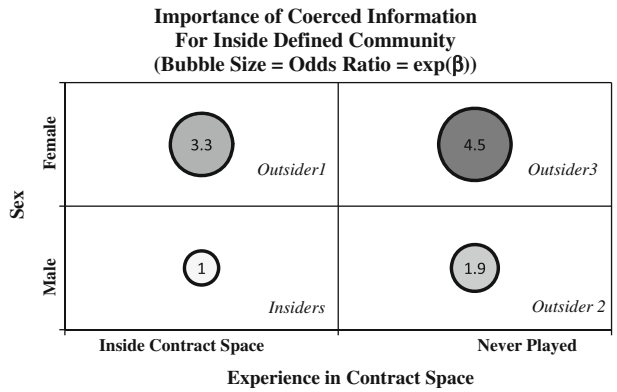

Fig. 1 Divergence of relative importance of coerced information: insider versus outsiders

This signifies the additional (if $\Delta\beta > 0$) privacy expectations afforded to close colleagues.

For example, the content of the information had different levels of importance across scenarios. Outsiders were consistent in assigning the role of "family" content in both an athletic team and less-defined team scenario, however, the weight of dating information changed significantly with an additional privacy expectation for less-defined team scenarios. While all content is associated with higher categories on the rating scale (more likely to rate closer to "Wrong to Share"), the coefficients for the less-defined team scenarios were 1.153 *greater than* those for the well-defined team thereby having greater expectations of privacy in a less-defined team contract space as compared to well-defined, norm-generating contract community.[10] A similar analysis can be done on the outsider groups who consistently give *greater* protections to dating, family, and medical information for less-defined team vignette scenarios as compared to well-defined team scenarios.

The findings support the prediction in Hypothesis 2a that individuals hold different authentic norms about privacy across contracting scenarios. Each contracting group appears to have taken into consideration different authentic norms about privacy for the well-defined contracting community as compared to the less-defined contract community vignette scenarios as illustrated in Table 3.

Hypothesis 2b predicts the difference between authentic norms within well-defined and less-defined contracting communities will vary between inside and outside contractors. To examine the third hypothesis, I compared the additional privacy expectations ($\Delta\beta$) in well-defined contracting communities as illustrated in Table 3. Aside from personal information, which is consistently given *less* protection in a well-defined contracting community, respondents do not project similar authentic norms onto a hypothetical contracting community—or do the differences even trend in a similar direction. In other words, insiders and outsiders diverge on the relative importance of privacy factors within the well-defined community.

More specifically, according to those most outside the community, insiders should have greater protections from coercion—the sharing of information is more likely to be considered wrong. Yet, insiders do not take coercion into consideration in either scenario as is illustrated in Fig. 2. Figure 2 shows the additional (if $\Delta\beta > 0$) protections given to well-defined community for each contracting group. The findings support the prediction in Hypothesis 2b that the difference between authentic norms within well-defined and less-defined contracting communities will vary between inside and outside contractors. In fact, those farthest away from the contracting community projected the greatest additional protections on coerced information and diverged the most from insiders of that contracting community.

Discussion and Conclusion

The findings of this study contribute to the literature on managing privacy expectations by examining whether and how authentic norms of privacy vary across particular contexts and groups of individuals. As such, the findings speak directly to the needs of organizations to manage a diverse set of privacy issues across stakeholder groups.

A social contract approach to privacy was supported by the findings in this study. *As hypothesized, authentic privacy norms were shown to vary based on a respondent's proximity to the contract community*. These findings illustrate the different privacy norms generated within communities as understood by insiders and outsiders and support the concept of a different set of privacy norms understood within a particular contract community. In addition, the results suggest contractors have distinct authentic privacy norms for particular groups of people or exchanges as privacy expectations varied across different contracting communities.

The results reported here challenge conventional views of how individuals form privacy expectations. Traditionally, management research has chosen a static definition of privacy across individuals and situations, wherein individuals, information, or locations could be declared either private or not private. However, in this study, individuals formed privacy norms dependent upon the contracting communities and relationships and *always* held expectations of privacy. These findings suggest that privacy can be more completely understood only when specific contract communities and authentic privacy norms are identified or

[10] For example, insiders see dating ($\Delta\beta = -1.707$), family (-1.163), and medical (-0.319) content as *more* "OK to Share" within the well-defined contracting scenarios as compared to the random team.

Table 3 Additional privacy expectations afforded to defined contract space

	Additional privacy protections $= \Delta\beta = \beta_a - \beta_b$							
	Contractors		Outsider 1		Outsider 2		Outsider 3	
	Model 1c		Model 2c		Model 3c		Model 4c	
	$\Delta\beta$	OR	$\Delta\beta$	OR	$\Delta\beta$	OR	$\Delta\beta$	OR
Access								
Coerced info		1.0	1.206	3.3	(0.120)	0.9	1.499	4.5
Overheard info							0.581	1.8
Willingly shared								
Content								
Role based					0.669	2.0		
Personal	(1.707)	0.2	(1.153)	0.3	(0.087)	0.9	(0.938)	0.4
Family	(1.163)	0.3	0.165	1.2	(0.113)	0.9	(0.019)	1.0
Private	(0.319)	0.7	(0.230)	0.8	0.835	2.3	(0.184)	0.8
Public								
Location								
Verbal outside			0.651	1.9				
e-mail								
FB feed	(0.833)	0.4			0.132	1.1	(0.598)	0.5
FB post	(1.463)	0.2	1.251	3.5	(0.503)	0.6	0.149	1.2
Verbal inside								
Distribution								
To leaders								
To captains			(0.705)	0.5			(0.474)	0.6
Outside group								
Inside group								
UG status	0.888	2.4	0.288	1.3	(0.144)	0.9	0.152	1.2

"what the meaning of information privacy is" (Smith et al. 1996).

The results support two general conclusions. First, individuals hold *different* privacy norms without necessarily having *diminished* expectations of privacy. In other words, just because an individual—a stakeholder, customer, user, employee, or a survey respondent—diverges from a predefined concept of privacy does not necessarily require the stakeholder to have *no* or *diminished* expectations of privacy. Individuals differed on the factors they considered important in calculating privacy expectations, yet all groups had robust, authentic privacy norms as evidenced by the

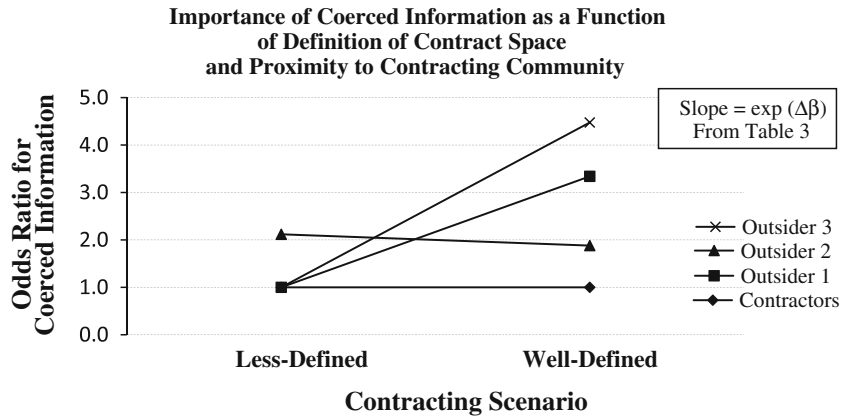

Fig. 2 Additional privacy protections within defined contract space

goodness-of-fit measures. Second, outsiders have difficulty projecting the authentic privacy norms of a contracting community. For managers and scholars, this renders privacy expectations more difficult to identify at a distance. These conclusions have implications for the scope and methods used in analyzing privacy in management. I discuss the theoretical and practical implications of both conclusions before addressing the study's strengths and limitations.

Implications for Scholarship

The findings have implications both how we ask the questions and the questions we ask in privacy scholarship. First, the research questions would change from *if* a person, situation, or information has an expectation of privacy to *what are* the privacy expectations of this community? What factors do contractors find important? Given a social contract approach to privacy, scholarship would focus on identifying the relevant contracting community, the benefits and harms of the particular exchange, and maintaining social contract minimums. This social contract foundation would form a platform for negotiating particular authentic privacy norms.

In addition, outsiders struggle to estimate the authentic norms of specific contracting communities (Dunfee 2006), and the findings support this argument. Yet, for research, much of our current privacy scholarship assumes a substantive theoretical definition of privacy on all contract spaces and tests for the degree to which respondents conform to a particular definition of privacy. The findings from this study would suggest that this tactic would be problematic. As noted by privacy scholar Nissenbaum, "most existing privacy surveys are of limited relevance because the way they frame their questions does not allow for a correspondence to be drawn between answers and the key parameters of informational norms" (2009, p. 150) as most studies test the respondent's adherence to a static and presumably universally accepted definition of privacy. For example, survey questions ask if respondents value or protect privacy as if privacy is universally understood (Oz 2001; Borna and Avila 1999). Or, more commonly, inconsistent survey results are found to be indicative of individuals having diminished concerns for privacy (Acquisti and Gross 2006; Culnan and Armstrong 1999), rather than the possibility that these respondents have different conceptions of privacy but an equal concern. Presuming a universal definition of privacy renders privacy easier to test, but misses the contextual effects of a given situation and limits the ability of individuals to hold different reasonable expectations of privacy across situations (Smith et al. 1996). Therefore, a social contract approach to privacy necessitates a methodological approach that offers participants a range of factors to consider in their privacy expectations and, therefore, changes how research is conducted.

For example, in a widely cited study, Smith et al. (1996) explain privacy in terms of location, content, secondary use, and accessibility (see also Mossholder et al. 1991; Milberg et al. 2000; Winter et al. 2004), and Table 3 contains these broad categories in the vignette factors. Previous work viewed these categories as mandatory components of a private situation rather than as areas of negotiation for authentic privacy norms. Yet, Smith et al. (1996) originally noted that the factors could vary and that inductive research may be necessary to understand the complexity of individuals' privacy norms. The findings here would suggest reframing previous static definitions of privacy as possible components of a social contract; such components would be neither necessary nor sufficient to explain privacy expectations but would perhaps guide negotiations around actual authentic information norms. Future work could develop a meso-level framework of privacy factors based on the findings of this study and current privacy research. This framework would constitute areas for negotiating an actual social contract or areas for analyzing hypothetical social contracts.

This study shows that insiders to a contracting community understand the privacy norms differently from outsiders. However, why privacy norms differ is not identified. As to the underlying reasons why these norms differ across hypothetical communities or across respondent types, it could be due to a reliance on different hypernorms or, if one is so inclined, a different understanding of *substantive* hypernorms, or based on a calculation of possible harms/benefits, or a different value placed on privacy. The survey instrument is agnostic to the underlying drivers. One thing was demonstrated here: that the differences were based on proximity to the contracting community rather than alternative demographics.

The difference in the privacy judgments across respondents and across communities could be due to not understanding the (a) relationships within the communities, (b) agreed upon norms within the contracting group, or (c) value of the information within that community. A social contract approach allows for differences based on all the three. Privacy norms are a product of the context, the specific actors, the information, and the type of flow of information (if it is expected, allowed, or impermissible) (Nissenbaum 2009); outsiders do not understand this combination. For the same community, a different piece of information may have different expectations of how the information will flow.

In addition, while not examined or emphasized here, the role of second-order norms or hypernorms should be targeted in future studies. The findings here leave open two possibilities for second-order norms that are found in theory. First, substantive privacy hypernorms may guide respondents and authentic privacy norms may reflect the specific manifestation of broader underlying principles—

whether they be hypernorms or second-order norms. Based on this approach to universal principles within social contract theory, future research may focus on what underlying principles individuals are *drawing on* in assessing whether it is appropriate to share information or not.[11] Second, some social contract theorists view second-order norms—in particular, any hypernorms that appear substantive—as based on the commonality of authentic norms (Walzer 2006); such scholars take a more inductive approach to the development of thin principles. Based on this second approach to hypernorms in social contract theory, future research may focus on what thin principles individuals are *developing* in assessing whether it is appropriate to share information or not. Finally, structural hypernorms may guide the negotiation of specific privacy norms with legitimate norms both abiding by the internal morality of contracting (Coase 1937; van Oosterhout et al. 2006) as well as the goals and purpose of the context (Nissenbaum 2009). While this study was specifically designed to remain agnostic as to the source of authentic privacy norms, future research could be designed to identify meso-level or second-order norms that transcend contexts, industries, or technology platforms.

While we have long known that *the degree an individual is concerned about privacy* differs based on experiences, personal characteristics, and type of information (Milberg et al. 2000; Culnan 1993; Malhotra et al. 2004), context-dependent approaches to privacy, as well as this study, go further to argue that the highly specific norms of appropriate information to disclose and distribute within a particular context is being determined by the individuals within a relationship or contract community. Privacy norms are not only influenced by the situation but also the factors that contribute to the definition of privacy are negotiated within communities.

If privacy expectations are composed of different factors with different weights depending on the specific contract community, then organizations will need to deploy different tactics to meet the privacy expectations of specific stakeholder relationships (Son and Kim 2008). If social contract norms govern an information space, then normative examinations would be more appropriate to understand the factors that contribute to the privacy expectations of consumers, employees, and users. Integrating ethical reasoning into these tactics and management techniques is important due to the difficulty in relying upon legal requirements in both firm–stakeholder relationships (Culnan and Williams 2009) and personal relationships (Rosen 2010). Respecting stakeholders' contextually dependent privacy expectations has both instrumental and intrinsic value (Johnson 2001): doing so respects the autonomy of users, stakeholder, and employees and is necessary for healthy relationships (Fried 1984) and exchange (Pavlau et al. 2007). Therefore, this study contributes to scholarship seeking to use ethical frameworks in the examination of privacy by offering a version of CBE to study privacy.

Implications for Practice

A social contract approach to privacy changes an organization's approach to managing privacy expectations of stakeholders. Given the divergent understandings of insiders and outsiders, managers will have difficulty in correctly projecting the specific privacy expectations of all consumers, employees, or users. In fact, arguments that employees, customers, and other stakeholders have no expectation of privacy for a given situation may be due to the difficulty outsiders have in identifying local norms.

The recent mismanagement of privacy changes within social network products, such as Google Buzz or Facebook, demonstrates the difficulty even experienced managers have in projecting the privacy norms of actual contractors. For managers, focus groups and qualitative or experimental surveys may be helpful to understand the privacy concerns of actual contractors. In addition, a recent call for dynamism in social contract approaches would be instructive for managers (Phillips and Johnson-Cramer 2006). Social contracts—both actual and hypothetical—are constantly evolving and need to be reevaluated regularly. Therefore, changes to privacy settings or defaults should not necessarily be viewed as failures on the part of organizations, but as an opportunity to renegotiate a social contract. The findings here would suggest that individuals are constantly negotiating authentic privacy norms within each contracting community—even with a random group of people on social networking sites. Such an approach is supported by Angst and Agarwal (2009) who demonstrated privacy attitudes and expectations can be modified through messaging and education: privacy expectations are malleable and evolve. Based on this study, these changes may be due to the evolving privacy norms within the contract community. In addition, the goal of organizations in managing privacy expectations would also change given the findings of this study. Importantly for managers, rather than determine if a given situation is private or not private, the focus would be on how a situation could meet privacy expectations of those involved. Not only do social contract moral minimums pervade all contract spaces but also authentic privacy norms are negotiated within those communities.

Two precepts of social contract theory limit the ability for managers to find situations, information, or individuals as having diminished or no expectations of privacy given a social contract approach to privacy. First, social contract

[11] I wish to thank an anonymous reviewer for pointing out this relationship between universal principles and the privacy norms found in this study.

approaches encompass both actual and hypothetical contracts as governing contract spaces. In other words, a social contract need not be written or spoken to have moral weight. Currently, privacy prescriptions focus on actual contracts when information is gathered—as is the case with Fair Information Practice's notice and consent stipulations or the restricted access version of privacy. For example, employees are notified of monitoring and click "OK" to consent; customers are notified of broad user tracking and shown lengthy privacy notices before choosing a service. In so doing, managers rely upon actual notice and consent as a way to meet privacy expectations, which has been argued to be ineffective in upholding expectations of privacy (Beales and Muris 2008). As such, managerial attention is too focused on actual contracts and should shift to the ongoing actual and hypothetical social contract governing the contract community for moral guidance concerning privacy norms.

Second, there exists an internal morality to social contracts in that social contracts necessitate both effective and mutually beneficial rules to be sustainable (van Oosterhout et al. 2006). The internal morality of contracting would suggest that privacy norms must (a) meet the needs of all contractors and (b) contribute to the effectiveness of the relationship or exchange. Current tactics for managers which rely upon the ability of organizations to "own" customer data and dictate subsequent use would breach the requirement of mutually beneficial rules and actions. In addition, guidance that focuses on rendering information inaccessible to employers, trading partners, or government agencies to maintain privacy may breach the requirement for rules and actions to be effective: individuals cannot trade without also exchanging information (Singleton 1998). As Nissenbaum (2009) notes, privacy norms must meet the goals and purpose of the particular context.

For example, employee monitoring can mistakenly be categorized as a necessary infringement of privacy where employees are forced to relinquish information as a condition of their employment. However, a social contract approach to privacy would suggest privacy norms *within the employer–employee relationship* must meet the needs of both parties and be effective over time. Therefore, privacy norms as to the type of information that is expected and allowed to be shared and what each party can do with the information must be effective to the working relationships and benefit the contractors. This argument is in keeping with Brenkert's (1981) framing of privacy expectations being developed for specific relationships such as doctor–patient or employer–applicant. Tracking phone calls and e-mails need not infringe of the privacy of either party if the tactics conform to the authentic norms of that relationship. However, the authentic privacy norms would also need to suit the purpose and goals of the community and conform to the structural hypernorms of social contract theory.

In addition, many jurisdictions have third party privacy standards that are applicable apart from the community-negotiated standards. For example, the Canadian Privacy Commissioner on Canada, Gramm Leach Bliley Act, COPPA, and HIPPA within the US, and the EU Data Protection Directive in Europe. Therefore, even if an organization successfully navigates contextual privacy norms, they must also comply with regulatory bodies.[12]

Going forward, managers would shift from actual notice and consent or claims of ownership and move to identify the relevant contracting community, ensure contractors have structural second-order norms, and develop authentic privacy norms that are sustainable by being mutually beneficial and effective.

Strengths, Limitations, and Suggestions

This research presents one of the first studies of CBE using the factorial vignette survey methodology. Previous empirical work within CBE has examined substantive hypernorms through the convergence of norms across contract groups thereby identifying hypernorms by areas of agreement. Yet substantive second-order hypernorms were not found in this study. As noted by van Oosterhout et al. (2006), the search for substantive hypernorms that transcend contract spaces and give definitive direction for contractors judgments and behaviors can be considered the contractualist fallacy. Therefore, future work could focus on structural or procedural second-order norms rather than search for a single set of action guiding norms or institutions.

Yet, social contract minimums—or structural hypernorms—were also not consistently significant to privacy expectations in this study. For example, consent of the protagonist in the story with the contract community and, presumably, with its negotiated authentic norms, was not a factor in any model. The operationalization of this consent as "new student" versus senior may have contributed to this finding. Operationalizing second-order norms has proven difficult across CBE and future work could identify methods to examine universal social contract norms. Supporting social contract minimums such as exit, voice, and informed consent is a viable direction for future privacy research.

In general, factorial vignette surveys provide a bridge between experiments and surveys (Wallander 2009) and, therefore, carry the strengths and weaknesses of both types of empirical work. The methodology captures the complexities of real decision making, since a large number of

[12] I wish to thank an anonymous reviewer for making this point.

contexts and conditions affecting judgments are systematically varied (Taylor 2006, p. 1196), 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 (Wallander 2009; Taylor 2006)—an important point when studying privacy and business ethics in particular. Individuals are not always able to identify and articulate the conditions or factors which influence their judgments as is necessary in other methodologies. Finally, compared to traditional survey research, factorial vignette surveys avoid non-orthogonal or collinear factors that occur in association with each other. The random combination of factors "ensures any non-orthogonality of the independent variables is due to random error only" (Taylor 2006, p. 1197).

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 found information "OK" or "Wrong to Share" (Taylor 2006). As noted in a recent review, factorial vignette survey methodology is unique in assuming an implicit agreement among individuals in a defined community as to what factors to consider when rendering a judgment (Wallander 2009, p. 514). However, in the analysis, pervasive cultural or personality differences may also explain the variances between contracting groups' responses. In the study's design, researcher bias can influence the inclusion of factors, and missing factors could change the final models for each group. 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 privacy violations.

Two pervasive issues with convenience samples were controlled during sensitivity testing of the models. First, the large and diverse sample for the control for undergraduate status. Undergraduate status was significant for all models *except* for insiders when assessing their own authentic norms and the third outsider group when assessing less-defined team scenarios. In addition, gender differences across privacy expectations, initially reported by Kuo et al. (2007), were supported more specifically in this study. Males were more likely to rate information as "OK to Share" (lower on the rating scale); female respondents were more likely to rate information as "Wrong to Share." As such, both student status and sex should be considered in future privacy studies.

Conclusion

This study demonstrated that privacy is a much more contextual and nuanced issue than previously theorized. Since privacy is an issue that underscores all stakeholder relationships, including employees, boards of directors, customers, suppliers, government, etc., new insights on privacy has direct practical implications for managers across industries. Privacy is integral to stakeholder management, to organizational trust, and to remain competitive in an increasingly information intense business environment.

Appendix

Vignette Factors

	Attributes	Dimensions		Operationalized
1	Space	0	Well defined—athletic team	*On a varsity athletic team*
		1	Ill defined—randomly assigned group	*On an assigned project team for a required class*
2	Access	0	Give willingly	
		1	Coerced	*[NAME]'s teammate only shared the information reluctantly after being chided by other students on the team*
		2	Overheard	*[NAME] was not sure that his teammate realized that he heard/received the information*
3	Content	0	Public	*Housing decisions for next semester*
		1	Role based	*Who is going to start for the next game/how the projects were assigned*
		2	Personal I	*A date that went horribly wrong*
		3	Family	*Problems with his mom*
		4	Private	*An embarrassing medical condition*

	Attributes	Dimensions		Operationalized
4	Location	0	Verbal inside role-based space	*While in the locker room/study room…heard*
		1	Verbal outside role-based space	*While in the cafeteria…heard*
		2	e-mail	*While checking his messages….received an e-mail*
		3	Facebook newsfeed	*While on Facebook…received a newsfeed*
		4	Facebook wall post	*While on Facebook…saw a wall post*
5	Distribution of information	0	Distributed within group	*Other members of the team*
		1	Distributed to team leaders	*Other members of the team including the coach*
		2	Distributed to captains	*Other members of the team including the team captains*
		3	Distributed outside group	*Students not on the team*
6	Membership	0	New	*New*
		1	Senior	*Senior*

Sample Vignettes

In general:

[NAME] is a [MEMBERSHIP] college student [SPACE]. [LOCATION A] [NAME] [LOCATION B] from a fellow team member talking about [CONTENT]. [ACCESS]. **The next day, [NAME] shared the information with [DISTRIBUTION]**

Sample 1: *Ryan is a senior college student on an assigned project team for a required class. While on Facebook, Ryan received a newsfeed from a fellow team member talking about problems with his mom. Ryan was not sure that his teammate realized that he saw the information.* ***The next day, Ryan shared the information with other students on the project team, including the professor.***

Sample 2: *Kevin is a new college student on a varsity athletic team. While on Facebook, Kevin saw a wall post from a fellow team member talking about a date that went horribly wrong. Kevin was not sure that his teammate realized that he saw the information.* ***The next day, Kevin shared the information with other members of the team.***

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy enhancing technology* (pp. 36–58).

Alder, G. S., Schminke, M., & Noel, T. W. (2007). The impact of individual ethics on reactions to potentially invasive HR practices. *Journal of Business Ethics, 75*(2), 201–214.

Allen, A. L. (1999). Coercing privacy. *William and Mary Law Review, 40*, 723.

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*(2), 339–370.

Appelbaum, L. D., Lennon, M. C., & Aber, J. L. (2006). When effort is threatening: the influence of the belief in a just world on Americans' attitudes toward antipoverty policy. *Political Psychology, 27*(3), 387–402.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*(2), 107–123.

Awad, N. F., & Krishman, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.

Bailey, W., & Spicer, A. (2007). When does National Identity Matter? Convergence and divergence in international business ethics. *Academy of Management Journal, 50*(6).

Beales, H. J., & Muris, T. J. (2008). Choice or consequences: Protecting privacy in commercial information. *The University of Chicago Law Review, 75*(1), 109–135.

Bennett, C. (1992). *Regulating privacy*. Ithaca: Cornell University Press.

Borna, S., & Avila, S. (1999). Genetic information: Consumers' right to privacy versus insurance companies' right to know a public opinion survey. *Journal of Business Ethics, 19*(4), 355–362.

Brenkert, G. (1981). Privacy, polygraphs, and work. *Business and Professional Ethics Journal, 1*, 23.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the doubleclick experience. *Journal of Business Ethics, 35*(4), 243–254.

Coase, R. H. (1937). The nature of the firm. *Economica, 4*(16), 386–405.

Culnan, M. J. (1993). How did they get my name? An exploratory investigation of computer attitudes toward secondary information use. *MIS Quarterly, 17*, 341–364.

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

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and tjx data breaches. *MIS Quarterly, 33*(4), 673–687.

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review, 19*(2), 252–284.

Donaldson, T., & Dunfee, T. W. (2002). Ties that bind in business ethics: Social contracts and why they matter. *Journal of Banking and Finance, 26*(9), 1853–1865.

Donaldson, T., & Dunfee, T. W. (1999). *Ties that bind: A social contract approach to business ethics*. Cambridge, MA: Harvard Business School Press.

Dunfee, T. W. (2006). A critical perspective of integrative social contracts theory: Recurring criticisms and next generation research topics. *Journal of Business Ethics, 68*(3), 303–328.

Elgesem, D. (1999). The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. *Ethics and Information Technology, 1*(4), 283–293.

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology, 8*(3), 109–119.

Fried, C. (1984). Privacy. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.

Ganong, L. H., & Coleman, M. (2006). Multiple segment factorial vignette designs. *Journal of Marriage and Family, 69*(2), 455–468.

Glac, K., & Kim, T. W. (2009). The "I" in ISCT: Normative and empirical facets of integration. *Journal of Business Ethics, 88*(4), 693–705.

Heugens, P. P. M. A. R., van Oosterhout, J., & Kaptein, S. P. (2006). Foundations and applications for contractualist business ethics. *Journal of Business Ethics, 68*(3), 211–228.

Husted, B. W. (1999). A critique of the empirical methods of integrative social contracts theory. *Journal of Business Ethics, 20*(3), 227–235.

Jasso, G. (1990). Factorial survey methods for studying beliefs and judgments. *Sociology Methods and Research, 34*(3), 334–423.

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

Jasso, G., & Opp, K. (1997). Probing the character of norms: A factorial survey analysis of the norms of political action. *American Sociological Review, 62*, 947–964.

Jiang, X., Hong, J. L., & Landay, J. A. (2002). Approximate information flows: Socially based modeling of privacy in Ubiquitous Computing, *Ubicomp 2002: ubiquitous computing* (pp. 176–193).

Johnson, D. (2001). *Computer ethics* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Johnson, D. (2004). Computer ethics. In L. Floridi (Ed.), *The Blackwell guide to the philosophy of computing and information* (pp. 64–75). Malden, MA: Blackwell.

Katz, N., & Koenig, G. (2001). Sports teams as a model for workplace teams: Lessons and liabilities. *Academy of Management Executive, 15*(3), 56–69.

Kennedy, P. (2003). *A guide to econometrics* (5th ed.). Cambridge, MA: MIT Press.

Kuo, F., Lin, C., & Hsu, M. (2007). Assessing gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics, 73*(2), 145–160.

Levitt, S. D., & List, J. A. (2007). What do laboratory experiments measuring social preferences reveal about the real world? *The Journal of Economic Perspectives, 21*(2), 153–174.

Lynch, J. (1982). The concept of external validity. *Journal of Consumer Research, 9*(3), 240–244.

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. (2010). Privacy revisited: From Lady Godiva's Peeping Tom to Facebook's Beacon Program. In D. E. Palmer (Ed.), *Ethical issues in e-business: Models and frameworks*. IGI Global: Hershey.

Martin, K., & Freeman, R. E. (2003). Some problems with employee monitoring. *Journal of Business Ethics, 43*, 353–361.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57.

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the Internet. *Journal of Business Ethics, 28*(3), 255–265.

Moor, J. (1997). Towards a theory of privacy in the information age. *Computers and Society, 27*, 27–32.

Mossholder, K. W., Giles, W. F., & Wesolowski, M. A. (1991). Information privacy and performance appraisal: An examination of employee perceptions and reactions. *Journal of Business Ethics, 10*(2), 151–156.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Standford, CA: Stanford University Press.

Nock, S., & Gutterbock, T. M. (2010). Survey experiments. In J. Wright & P. Marsden (Eds.), *Handbook of survey research* (2nd ed.). Amsterdam: Elsevier.

O'Connell, A. A. (2006). *Logistic regression models for ordinal response variables*. Thousand Oaks, CA: SAGE.

Oz, E. (2001). Organizational commitment and ethical behavior: An empirical study of information system professionals. *Journal of Business Ethics, 34*(2), 137–142.

Pavlau, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105–136.

Persson, A. J., & Hansson, S. O. (2003). Privacy at work—ethical criteria. *Journal of Business Ethics, 42*(1), 59–70.

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics, 59*(4), 327–345.

Phillips, R. A., & Johnson-Cramer, M. E. (2006). Ties that unwind: Dynamism in integrative social contracts theory. *Journal of Business Ethics, 38*(3), 283–302.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*(3), 221–235.

Rachels, J. (1975). Why is privacy important? *Philosophy & Public Affairs, 4*(4), 323–333.

Robertson, D. C., & Ross, W. T. (1995). Decision-making processes on ethical issues: the impact of a social contract perspective. *Business Ethics Quarterly, 5*(2), 213–240.

Rosen, J. (2010). The Web means the end of forgetting. *The New York Times*, July 21, 2010. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all.

Rossi, P., & Nock, S. (Eds.). (1982). *Measuring social judgments: The factorial survey approach*. Beverly Hills: SAGE.

Schoeman, F. (Ed.). (1984). Privacy: Philosophical dimensions of the literature. In *Philosophical dimensions of privacy: An anthology*. Cambridge: Cambridge University Press.

Shaw, T. R. (2003). The moral intensity of privacy: An empirical study of Webmaster' attitudes. *Journal of Business Ethics, 46*(4), 301–318.

Singleton, S. (1998). Privacy as censorship. *Cato Institute: Policy Analysis, 295*, 1–32.

Smith, H. J. (2004). Information privacy and its management. *MIS Quarterly Executive, 3*(4), 291–313.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review, *MIS Quarterly, 35*(4), 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Smith, N. C., Simpson, S. S., & Huang, C. (2007). Why managers fail to do the right thing: An empirical study of unethical and illegal conduct. *Business Ethics Quarterly, 17*(4), 633–667.

Smith, W. P., & Tabak, F. (2009). Monitoring employee e-mails: Is there any room for privacy? *Academy of Management Perspectives, 23*(4), 33–48.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477.

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503–529.

Soule, E. (2002). Managerial moral strategies—in search of a few good principles. *Academy of Management Journal, 27*, 114–124.

Spicer, A., Dunfee, T. W., & Bailey, W. J. (2004). Does national context matter in ethical decision making? An empirical test of integrated social contracts theory. *Academy of Management Review, 47*(4), 610–620.

Straub, D. W., & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly, 14*(2), 143–156.

Strong, K. C., & Ringer, R. C. (2000). An examination of integrative social contracts theory: Social hypernorms and authentic community norms in corporate drug testing programs. *Employee Responsibilities and Rights Journal, 12*(4), 237–247.

Tavani, H. T. (2008). Floridi's ontological theory of informational privacy: Some implications and challenges. *Ethics and Information Technology, 10*(2/3), 155–166.

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

Thompson, J. A., & Hart, D. W. (2006). Psychological contracts: A nano-level perspective on social contract theory. *Journal of Business Ethics, 68*(3), 229–241.

Thurman, Q. C., Lam, J. A., & Rossi, P. H. (1988). Sorting out the cuckoo's nest: A factorial survey approach to the study of popular conceptions of mental illness. *The Sociological Quarterly, 29*(4), 565–588.

Van de Hoven, J. (2008). Information technology, privacy, and the protection of personal data. In J. Weckert & J. Van de Hoven (Eds.), *Information technology and moral philosophy* (pp. 301–321). Cambridge: Cambridge University Press.

van Oosterhout, J., Heugens, P., & Kaptein, M. (2006). The internal morality of contracting: Advancing the contractualist endeavor in business ethics. *Academy of Management Review, 31*(3), 521–539.

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

Walzer, M. (2006). *Thick and thin: Moral argument at home and abroad*. South Bend, IN: University of Notre Dame Press.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Weber, J. (1992). Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly, 2*(2), 137–160.

Wempe, B. (2005). In defense of a self-disciplined, domain-specific social contract theory of business ethics. *Business Ethics Quarterly, 15*(1), 113–135.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Winter, S. J., Stylianou, A. C., & Giacalone, R. A. (2004). Individual differences in the acceptability of unethical information technology practices: The case of Machiavellianism and ethical ideology. *Journal of Business Ethics, 54*(3), 275–296.