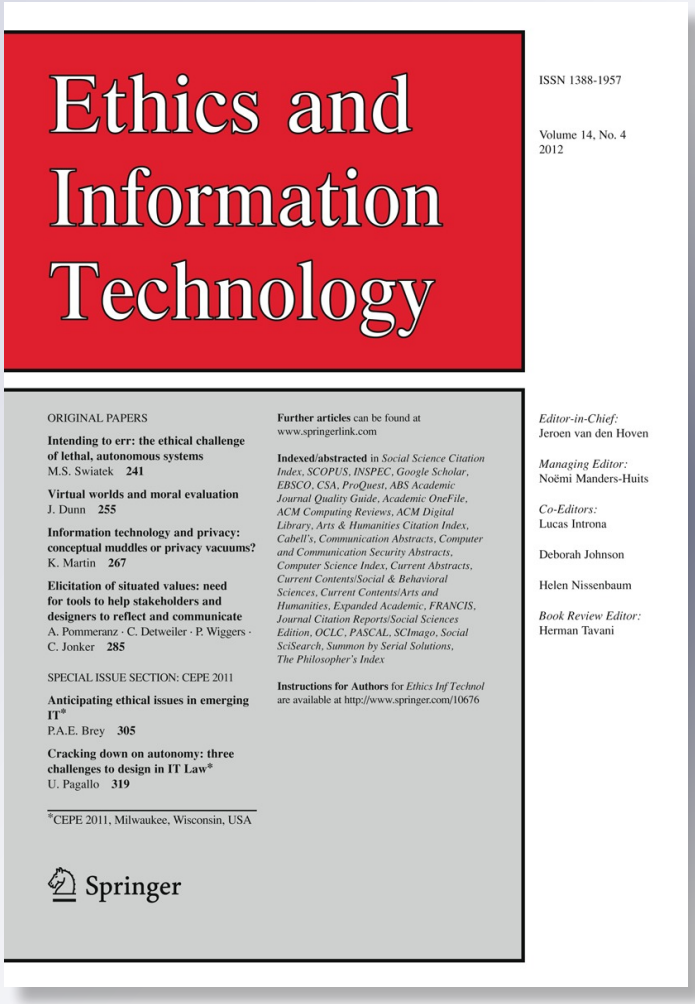
Information technology and privacy: conceptual muddles or privacy vacuums?

Kirsten Martin

Ethics and Information Technology

ISSN 1388-1957
Volume 14
Number 4

Ethics Inf Technol (2012) 14:267-284
DOI 10.1007/s10676-012-9300-3



Springer

Ethics Inf Technol (2012) 14:267–284
DOI 10.1007/s10676-012-9300-3

ORIGINAL PAPER

Information technology and privacy: conceptual muddles or privacy vacuums?

Kirsten Martin

Published online: 15 September 2012

Abstract Within a given conversation or information exchange, do privacy expectations change based on the technology used? Firms regularly require users, customers, and employees to shift existing relationships onto new information technology, yet little is known as about how technology impacts established privacy expectations and norms. Coworkers are asked to use new information technology, users of gmail are asked to use GoogleBuzz, patients and doctors are asked to record health records online, etc. Understanding how privacy expectations change, if at all, and the mechanisms by which such a variance is produced will help organizations make such transitions. This paper examines whether and how privacy expectations change based on the technological platform of an information exchange. The results suggest that privacy expectations are significantly distinct when the information exchange is located on a novel technology as compared to a more established technology. Furthermore, this difference is best explained when modeled by a shift in privacy expectations rather than fully technology-specific privacy norms. These results suggest that privacy expectations online are *connected* to privacy offline with a different base privacy expectation. Surprisingly, out of the five locations tested, respondents consistently assign information on email the greatest privacy protection. In addition, while undergraduate students differ from non-undergraduates when assessing a social networking site, no difference is found when judging an exchange on email. In sum, the findings suggest that novel technology may introduce temporary conceptual muddles rather than permanent privacy vacuums. The results reported here challenge conventional views about how privacy expectations differ online versus offline. Traditionally, management scholarship examines privacy online or with a specific new technology platform in isolation and without reference to the same information exchange offline. However, in the present study, individuals appear to have a *shift* in their privacy expectations but retain similar factors and their relative importance—the privacy equation by which they form judgments—across technologies. These findings suggest that privacy scholarship should make use of existing privacy norms within contexts when analyzing and studying privacy in a new technological platform.

Keywords Contextual integrity · Privacy · Business ethics · Information technology · Email · Facebook

K. Martin (✉)
School of Business, The George Washington University, Funger Hall, 2201 G St, NW, Washington, DC 20052, USA
e-mail: martink@gwu.edu

Technology complicates privacy research (Smith et al. 2011) and has consistently been an impetus for new privacy law, scholarship, and policy (Calo 2010). Information technology changes the flow of information (Johnson 2004), alters the user experience (Calo 2010), and adds an additional level of uncertainty (Hui et al. 2007). In short, information technologies challenge the rules that govern information flow, rendering privacy a consistent concern particularly online (Angst and Agarwal 2009; Hui et al. 2007).

A general assumption underlying information privacy scholarship is that new technologies lead to new privacy norms and expectations, thereby requiring research to develop along parallel lines for each new technology domain (Smith et al. 2011). Such parallel streams of privacy research are assumed to be necessary because the new technology—email, social networking sites, online retail,

etc.—does not necessarily support the established expectations of privacy. These presumed *privacy vacuums* created by the introduction of technology are areas where reasonable individuals have diminished or even no reasonable expectations of privacy, and the novel technology is assumed to be void of privacy norms [e.g., social networking sites (Acquisti and Gross 2006), email (Weisband and Reinig 1995)]. Nissenbaum (2004) refers to these hypothetical privacy vacuums as the 'anything goes fallacy'—the mistaken belief that contexts, spaces, or situations exist without privacy expectations.

It remains unclear if distinct privacy norms and parallel research streams are required for the introduction of novel technology. Instead, technology may introduce *conceptual muddles* (Moor 1985) or disruptions (Calo 2010) where society takes a moment to absorb the novel technology due to confusion or uncertainty. As noted in a review by Awad and Krishman (2006), most empirical privacy studies focus on either offline or online information exchange without directly comparing privacy expectations and norms across technology platforms. Privacy and information technology empirical research has paid little attention to such contextual differences and specific privacy beliefs across technology (Malhotra et al. 2004: 349). The theoretical scholarship is ambivalent as to the novelty of values and norms due to the introduction of technology with arguments for both temporary conceptual muddles and permanent privacy vacuums within privacy scholarship.

The goal of this study is to empirically examine whether and how privacy expectations differ based on the technological platform of the information exchange. To examine the manner in which privacy expectations change based on the technological platform, factorial vignette survey methodology is used (Rossi and Nock 1982; Jasso 1990). In this study, 471 respondents rated 15,108 vignettes and judged if the protagonist in the hypothetical situations was *Wrong to Share* the information. The research presented here isolates whether and how respondents' privacy expectations differ across technology platforms controlling for all other aspects of the exchange including the context of the relationship, the recipient of the information, and the type of information. The results are theoretically generalizable as the design tests alternative theories as to how technology impacts privacy expectations and norms. The findings from this experimental study identify the model that best explains the conceptual relationship between technology and privacy expectations (Levitt and List 2007).

This design mitigates three concerns in privacy research. First, privacy research is fraught with respondent bias where respondents inflate their concern for privacy which may not reflect their true attitude (Hui et al. 2007). For example, despite a reported general concern for internet privacy, users seldom provide false information or alter their privacy settings (Acquisti and Gross 2006). The factorial vignette survey methodology is specifically designed within sociology to avoid respondent bias by indirectly measuring the privacy factors and their relative importance of respondents informing normative judgments. Second, respondents may not agree with a theoretical definition of privacy while still retaining privacy expectations. Privacy is a complicated phenomenon requiring sophisticated techniques to examine individual responses to privacy violations within specific contexts (Malhotra et al. 2004). This study focused on the differences in privacy expectations across technologies and not whether or not the respondents agree with a theoretical definition of privacy. The method allows for privacy norms to differ without necessarily being diminished by decoupling the privacy factors and their relative importance for a specific context with the judgment that the information is wrong to share. Finally, the rating task captures the judgment of respondents and not actual laws or privacy policies; recent research has suggested the importance of focusing on privacy expectations rather than regulations or stated policies because most privacy issues can and should be addressed through ethical analysis (Culnan and Williams 2009; Nissenbaum 2004).

The research reported here makes several contributions to research and practice. First, organizations regularly ask individuals to move relationships and information exchanges across technology platforms. Coworkers are asked to use new information technology, users of gmail are asked to use GoogleBuzz, patients and doctors are asked to record health records online, etc. Understanding how privacy expectations theoretically change, if at all, and the mechanisms by which such a variance is produced will help organizations make such transitions. Second, directly examining privacy expectations across technologies may explain why scholars struggle to connect the online exchange of information to offline relationships. While a connection has been suggested in theory (Johnson 2004; Nissenbaum 2009), any link across online and offline privacy expectations is rarely directly examined in research (Awad and Krishman 2006). However, this study directly compares the same exchange of information across different locations or technology platforms holding the actors, information, and the situation constant to isolate the effect of the technology.

Theoretical foundation and hypotheses development

Before empirically examining whether and how privacy norms and expectations change across technology platforms, a general model of privacy expectations is developed by leveraging two areas of privacy scholarship focusing on

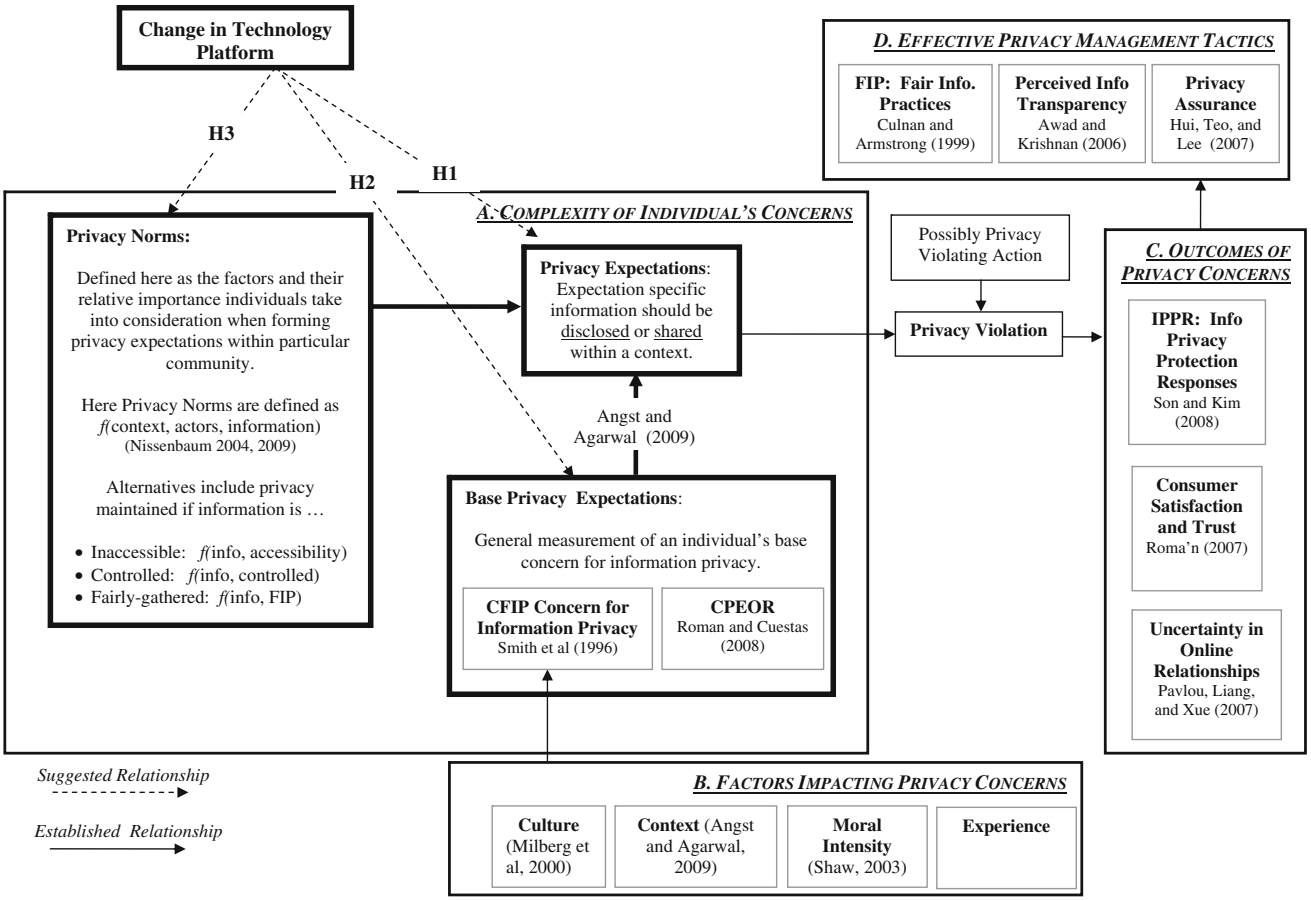


Fig. 1 What we know and measure about privacy & technology

(1) individual-specific base privacy concerns and (2) contextually-defined privacy norms. Figure 1 depicts how base privacy concerns, contextually defined privacy norms, and privacy expectations fit within the larger picture of privacy research.

One stream of privacy scholarship seeks to identify individual-specific disposition or concerns towards privacy. For example, an individual's concern for information privacy, or CFIP, is measured through a context-independent survey instrument developed by Smith et al. (1996). Similar measurements include an individual's willingness to provide personal information to transact (Dinev and Hart 2006) or their general information privacy concerns (Malhotra et al. 2004). Each instrument measures an individual's conformance to a view of privacy (as defined by the scholars) to produce a general disposition towards privacy. This privacy concern is a factor of prior experience and personality suggesting a static privacy expectation attributable to specific individual as depicted in Fig. 1.

Yet individuals do not act in conformance with their stated concern for information privacy suggesting additional factors are taken into account in forming privacy judgments (Smith et al. 2011). In addition to a base privacy expectation, individuals consider the established privacy norms or the agreed upon rules that also govern expectations of privacy. These rules are the factors and their relative importance individuals take into consideration in assessing privacy. For example, one strain of scholarship assumes privacy is a function of the accessibility of the information; information that is inaccessible is considered private and information that is accessible is considered public (Schoeman 1984; Posner 1981).

An additional set of privacy norms supplements the base privacy concerns as illustrated in the bolded boxes in Fig. 1. Below, Model 0 allows for individual level base expectations or concerns as well as a set of commonly held privacy norms. For any individual *i*, we would find the following model for a given set of privacy factors:

$$(0) \quad \text{Privacy Expectations}_i = \text{Base Expectations}_i + \text{Privacy Norms}$$

Yet, privacy norms are not universally defined, thereby only adding to the ambiguity in privacy scholarship. Privacy remains a fuzzy concept in general (Van de Hoven 2008) and has proven difficult to empirically examine due

to the different approaches to the very definition of privacy. Privacy has been viewed as

- a function of the control over information (Westin 1967; Margulis 1977; Altman 1975; Moor 1997) where privacy norms = *f*(information, controlled).
- a function of the fairness of the exchange (Culnan and Armstrong 1999) where privacy norms = *f*(information, fairness or FIP).
- or a function of the accessibility of information (Schoeman 1984; Posner 1981) where privacy norms = *f*(information, accessibility).

Privacy need not be considered a single entity with a one-size-fits-all definition (Smith et al. 2011). Within a growing field of contextually-defined privacy approaches, what is and is not private is dependent upon the relationships, actors, information, and context (Nissenbaum 2004, 2009; Solove 2006; Grimmelmann 2010; Tufekci 2008; Martin 2012). The rules used to develop privacy norms vary across contexts, and violations of privacy occur when these negotiated, context-dependent rules are broken. In other words, the vary function of privacy norms is negotiated within a context.[1] For example, it has become almost cliché to declare young adults to have diminished or no privacy expectations, yet, when examined closely, young adults are found to have negotiated privacy norms that differ from older adults while retaining strong expectations of privacy (Hoofnagle et al. 2010). Young adults have developed *different* privacy norms within their communities while still retaining expectations of privacy.

More specifically, the type of information, the actors in the context, and the purpose of the context all come into consideration when deciding whether receiving or sharing information is within privacy expectations (Nissenbaum 2004, 2009). For example, family information willingly shared with a colleague in a public area may reasonably be expected to be kept private within that conversation. However, change one aspect of the context—the type of information, the manner in which it was disclosed, the recipient, the location—and the rules governing the expectations of privacy may change. Below, Model 0 is modified to account for such contextually dependent approaches to privacy that allow privacy norms and privacy expectations to vary across contexts, relationships, information type, or technology platforms and where privacy norms are a function of the context, information, and actors. Therefore, for individual i, privacy expectations are comprised of the individual's base privacy expectations and the privacy norms of the context as in Model I.

$$(1)\quad \text{Privacy Expectations}_i = \text{Base Expectations}_i + f(\text{Context}, \text{Actors}, \text{Information})$$

The research question addressed in this study is whether and how technology impacts privacy expectations and norms as depicted in Model I above. The hypotheses below examine (1) theoretical differences in privacy expectations across technology platforms in addition to (2) the mechanisms by which these differences in expectations are produced using Model I.

Theoretically, computer technology enables different human actions, and humans not only can do new activities with technology, but individuals can do the same sorts of things in new ways (Johnson 2004). Johnson's introduction of action theory to the ethical analysis of technology suggests technology is neither immaterial nor deterministic in the actions individuals perform; rather, technology enables new actions (act tokens) that have varying degrees of familiarity to existing general types of acts (act types). Individuals may converse in person or talk over the phone and remain reasonably certain that both act tokens are part of the same act type (talking between friends). However, technology can also enable a novel act token to become disassociated from a known act type. Consider a uniformed police officer listening to a witness in a police station compared to the same officer using a listening device to listen to someone in their home. The second act token has become disengaged from the act type 'listening' with the introduction of a novel technology platform and with implications to possible new privacy norms and expectations governing that exchange. These new act tokens, enabled by novel technology, have properties that are both similar to and distinct from other tokens of the same act type. How distinct and how similar will depend on the technology used in the exchange of information and is examined in Models II–IV and Hypotheses 2–4 below.

The following sections describe the theoretical and operational foundations of the models. Importantly for this study, and given Eq. I above, the privacy norms and expectations may be (a) quite similar with little distinction across technologies, (b) differ across a base expectation yet have common privacy norms, (c) share a base expectation but differ on the privacy norms, or (d) be fully disengaged from the governing act type with novel base expectations and privacy norms. These possibilities are depicted by arrows H1–H3 in Fig. 1 and will be explained by Models I–IV.

[1] This negotiation over privacy norms is not synonymous with privacy as a commodity (Smith et al. 2011), a privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006), or a second exchange (Culnan and Bies 2003), all of which assume individuals *relinquish* privacy in order to gain something in return. In other words, individuals are seen as giving up some measure of privacy to benefit from a transaction (e.g., customizing products or using electronic health records or having books suggested online). In this paper, the negotiation is over the privacy norm function; actors within a context negotiate what the privacy rules will be while retaining every expectation of privacy.

Technology gap

In order to compare privacy expectations across technology platforms, both the novelty of the technology (Moor 1985) and the information friction of the technology (Floridi 2006a, b) are argued to be theoretically important. First, Moor (1985) refers to normative differences across technologies as conceptual muddles where values lag—sometimes just temporarily—behind technological advances. For example, while all online exchanges of information increase uncertainty (Pavlou et al. 2007), social networking sites are known as being exceptionally uncertain with unknown impacts on privacy due to the unfamiliarity of the technology (Hull et al. 2010). This would suggest that a *novel* technology application would have different privacy expectations in comparison to more established locations such as in a public space or email.

Therefore, one theoretical possibility posits that more novel technology has lower privacy expectations with fewer norms for guidance, thereby rendering information more likely to be expected to be shared. Generally, the technology platform of the information exchange will impact the privacy expectations, and more specifically, locating the information exchange on a novel technology platform will decrease the privacy expectation of individuals—information will be more likely to be expected to be shared.

Hypothesis 1a All other things being equal, locating the information exchange on a technology platform that is novel will decrease the privacy expectations of individuals—information will be more likely to be expected to be shared.

A second theoretical argument claims that technology features have a fundamentally different meaning in the offline setting than in the online setting (Awad and Krishman 2006), thus suggesting the shifts or differences in privacy expectations across technologies are more permanent. Specifically, Floridi (2006a, b) identifies the information friction—the degree to which information can be easily distributed—as a major factor in calculating privacy expectations. Technology that renders information easily seen or transmitted—e.g., a Facebook Post or an email—would have lower information friction than the same information exchange in a private room where information is less greased or easily shared (Moor 1997).

Rather than focusing on the uncertainty or trust in the technology, this line of scholarship weighs the physical environment or architecture as important in forming privacy expectations: greater information friction supports greater privacy expectations. Therefore, in this study, technology that allows information to be easily distributed would be associated with less information friction and a greater proportion of information being expected to be shared.

Hypothesis 1b All things being equal, locating the information exchange on a technology platform that allows information to be easily seen or shared will decrease the privacy expectation of individuals—information will be more likely to be expected to be shared.

Mechanism of privacy difference across technologies

The second set of hypotheses examines the mechanism by which any technology gap—the variance in the privacy expectations due to the technology platform—is produced. Where hypothesis 1 examines if a change in technology produces different privacy expectations as depicted in the arrow H1 in Fig. 1, the second set of hypotheses examine how that difference is produced given Model I above.

Model II hypothesizes a theoretical *shift* in the privacy expectations; the factors we take into consideration may be consistent across locations, but novel technologies provide a change in base expectations (Tavani 2008; Moor 1985) as depicted by arrow H2 in Fig. 1. In other words, while technology may introduce a change in the overall privacy expectations, communities have existing norms around a general type of act—e.g., sharing information with a colleague—which could provide guidance around a very specific and novel action—e.g., sharing information with a colleague through email. Research on the concern for information privacy (Smith et al. 1996) regularly examines the respondents' privacy concern across contexts which would suggest a respondent-level base privacy expectation within contexts (Malhotra et al. 2004) with a certain portion of which can be influenced by changes in technology (Dinev and Hart 2006).

Therefore, Model II suggests technology introduces a shift in the base privacy expectations of individuals due to the uncertainty of the environment or the lack of trust of the technology (Hui et al. 2007) while retaining the overall privacy norms of the relationship. For example, the type of information may be equally important in two locations—on email and in a private room—but the expectations that the information will not be shared is shifted in one location. For each technology t, Model II would suggest a technology-factor would shift the technology-specific *base expectations* while more specific privacy factors—such as the type of content used to calculate privacy expectations—would be constrained to be consistent across technologies.

$$\text{(II)}\quad \text{Privacy Expectations}_t = \text{Base Expectation}_t + f(\text{Context}, \text{Actors}, \text{Information})$$

Hypothesis 2 Differences in privacy expectations across technology platforms will be explained by a shift in the technology-specific base expectations (Model II).

Model III hypothesizes that individuals may start with similar base expectations but technology influences the privacy factors and their relative importance that individuals take into consideration in forming privacy expectations as depicted by arrow H3 in Fig. 1. Researchers regularly examine privacy online due to the persistence, searchability, and cross-indexibility of information (Tufekci 2008) or the decreased information friction of the context (Floridi 2006a, b) as influencing privacy norms. This line of scholarship suggests that different technology necessitates novel privacy norms due to the physical environment of the information. For example, the type of content may be more important in email as opposed to a public space or the recipient of information may be more context sensitive in email as opposed to a social networking site. For each technology t, privacy expectations would be comprised of a constrained base expectation with a technology-specific privacy norms as in Model III below.

$$\text{(III)}\quad \text{Privacy Expectations}_t = \text{BaseExpectation} + f_t(\text{Context}, \text{Actors}, \text{Information})$$

Hypothesis 3 Differences in privacy expectations across technology platforms will be explained by different privacy factors and their relative importance (Model III).

Model IV hypothesizes that the privacy equation may be fully differentiated across technological platforms (see H4 in Fig. 1). In the language of Johnson's (2004) use of action theory, the act token introduced by a novel technology may become disengaged from the known act type. Therefore, it is possible that actions facilitated by a new technology become disassociated from a known contextual privacy norm. This would be the fully technology-specific model in Model IV. For each technology t, privacy expectations would be comprised of a technology-specific base expectation as well as privacy norms specific to each technology.

$$\text{(IV)}\quad \text{Privacy Expectations}_t = \text{BaseExpectation}_t + f_t(\text{Context}, \text{Actors}, \text{Information})$$

Hypothesis 4 Differences in privacy expectations across technology platforms will be explained by both a shift in the technology-specific base expectations as well as different weights of the privacy factors (Model IV).

Methods

The goal of this study is to examine the theoretical suggestion that privacy expectations differ across technology platforms. The objective of this study was to identify *whether* and *how* privacy expectations differ when an exchange of information changes location—e.g., from a private room to email and to a social networking site—and the mechanisms by which that difference is generated.

This is a proof-of-concept examination—a theoretical examination (Lynch 1982)—therefore the findings will support or not support the hypothesized models of how technology impacts privacy expectations and norms. Such research 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 identify the model that best explains the conceptual relationship between technology and privacy expectations (Levitt and List 2007).

The factorial vignette survey methodology, developed to investigate human judgments (Rossi and Nock 1982; Jasso 2006; Wallander 2009), was employed. 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).[2] 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). These factors and their associated coefficients are the *equations-inside-the-head* (Jasso 2006) of respondents and, herein, would constitute the norms of privacy depicted in Models I through IV above.

Vignette factors

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

[2] 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).

have relatively simple mappings onto the constructs of concern" (Lynch 1982, p. 233). Here, factors are representatively sampled in order to test the hypotheses.

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). 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. Based on the hypotheses developed, the study must include (1) different technologies or 'locations' for the vignettes and (2) privacy factors that may vary in importance across locations. The "Appendix" contains the vignette factors as well as a sample vignette.

Location

To examine whether and how privacy expectations differ across technological platforms, the information exchange described in the vignette varied in location. The vignettes included information that was shared in a small room, in a large public space such as a cafeteria, through email, through a Facebook Feed, and on a Facebook Post. The purpose of the study was to compare technology-focused contexts (e.g., email and Facebook) as compared to non-technology-focused contexts (e.g., verbally), this factor is referred to as 'Location' throughout the analysis to signify a change in location for the same information exchange. The factors included supported the overall privacy expectations to be examined across an established space (e.g. verbally in a public and private room), a non-novel information technology (e.g., email), and a novel information technology (e.g., Facebook) to cover both a theoretical novel and non-novel technology as theorized in hypotheses 1a. In addition, these five locations cover theoretical extremes in information friction—or the ease with which information can easily be shared or seen—as theorized in hypothesis 1b: verbal exchange in a private room represents a high information friction environment whereas email or a Facebook Feed represents a low information friction environment (Floridi 2006a, b).

Privacy factors

In addition to the technology platform described above, the explanatory variables in this study are the privacy factors in the vignettes. These factors and their relative importance constitute the privacy norms in the model above [e.g., $f(\text{Context}, \text{Actors}, \text{Information})$]

Across privacy definitions, the type of information is a consistent factor taken into account in developing privacy expectations: e.g., the accessibility of information, the fairness in receiving information (Culnan and Armstrong 1999), or the control over information (Westin 1967). Information privacy scholarship identifies privacy as being associated with a piece of information—e.g., information that is inaccessible is deemed private or information that is owned by an individual is considered private—and this study examines how the privacy expectations around particularly sensitive information may actually vary across technology platforms. Information protected in one context may be expected to be shared in another.[3]

To compare the privacy norms across technology platforms for hypotheses 2–4, two measurements of the type of information are isolated in this research: the sensitivity of the content (defined a priori the study) and the appropriateness of the initial disclosure of information (defined within the study by respondents).

Sensitive information Two types of sensitive information were included in the vignettes: both medical information about the protagonist as well as information about a family member. For comparison, non-sensitive information was included such as information that was widely known.

Wrong to disclose Respondents were asked if the information was wrong to initially disclose. While the outcome variable of this study focuses on the judgment that information is expected or wrong to be shared, individuals also make judgments about the initial disclosure of information, where information can be deemed inappropriate for a given recipient or context (Nissenbaum 2004; Floridi 2006a). The rating (0/1) was used as a factor in the analysis to examine if individuals ever find information wrong to disclose but also judge the same information appropriate to share. This captured the subjective assessment of the information under consideration and was used to analyze contexts where information deemed wrong to disclose is also protected by being judged wrong to share.

Many factors are taken into consideration when formulating privacy expectations, including the actors, the type of information, the manner in which information is disclosed,

[3] Individuals regularly give access to information to people or organizations while keeping the same information from others. Alternatively, the restricted access version of privacy—where information that is inaccessible is private and that which is accessible is public –supports a dichotomy where information can be universally declared 'public' or 'private.' Many find the distinction to be false (Solove 2006; Nissenbaum 2004, 2009; Tufekci 2008) and "the idea of two distinct spheres, of the 'public' and the 'private' is in many ways an outdated concept" (Marwick et al. 2010). Or, as Nissenbaum states, "the crucial issue is not whether the information is private or public, gathered from private or public settings, but whether the action breaches contextual integrity" (2004, p. 134).

and the context of the exchange (Nissenbaum 2004, 2009), and both the general context of the exchange and the type of recipients were included in the vignette (see "Appendix" for design and sample vignette). For example, vignettes varied on how the information was accessed—information was willingly shared, coerced, or overheard. In addition, the individuals in the vignettes were either colleagues or mere acquaintance. These factors added realism to the vignettes and were randomly assigned to the vignettes so that an equal proportion of each was assigned to the respondent sample. These additional factors decrease the probability of respondent bias: the vignettes included multiple simultaneously changing factors and the respondents have difficulty identifying exactly what is being tested. In addition, these additional factors allow the results to focus on the impact of technology on privacy norms and expectations across a wide range of information exchanges. In other words, the results speak to exchanges across many types of relationships and disclosures.

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 ($1{,}200 = 2 \times 3 \times 5 \times 5 \times 4 \times 2$). For factorial vignette surveys, the number of vignettes is typically set at 10-60 vignettes for each respondent to answer; this survey had respondents answer 40 vignettes. 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.[4]

Sample

The sample was recruited via e-mail within a single institution using heads of departments and teams as the primary contacts who forwarded the survey to their members. Both students and non-students were recruited: 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 of 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 1 (*OK to Share* information) to 3 (*Wrong to Share* Information) (Nissenbaum 2004).[5]

Analysis

The data in this study was in two levels: the vignette level factors and the respondent level control variables. For the larger survey, 811 respondents rated a range of 1–40 vignettes resulting in 21,187 rated vignettes or observations. This particular study restricted attention to those who rated over 20 vignettes due to the type of analysis conducted below; 471 respondents and 15,108 vignettes are used in the analysis below.[6]

In testing the hypotheses, ordinal regression was used to identify the factors that influence the privacy expectations of respondents across locations. 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

[4] Respondent fatigue was a factor for some respondent groups. Two dummy variables were created 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. all vignette ratings were discarded with a sequence number of 1 or 2 for the entire analysis.

[5] The rating task in the survey was a five-level ordinal scale (0–4) as is shown in the "Appendix", however the distribution of the ratings was not normal around the mean. The top three levels (0–2) were combined to create a new scale with three levels coded 1–3. The user was not, however, given an option to answer "I don't know" or "I need more information." The user could skip a vignette and continue.

[6] In order to examine respondent level factors with OLS regression equations *for each respondent*, a minimum number of ratings per respondents was required. Therefore, all respondents were dropped who answered less than 20 vignettes and removed their ratings from the larger data set of vignette ratings. Therefore, the number of respondents used in this study is 471 (rather than 811) and the total number of vignette rated is 15,108 (rather than 21,187).

Squares (OLS) regression models.[7] Strong associations between explanatory variables and ratings are represented by coefficients farther away from 0.0 to odds ratios farther away from 1.0 (since OR = exp(β)). A negative (positive) coefficient would have an odds ratio less (greater) than one and would signify the associated explanatory variable would have an upward (downward) impact on the rating task.

Let N be the number of respondents and K the number of vignettes. Thus in a multilevel framework, there are N units with level 2 demographic variables and K units with level 1 factor variables. The general ordinal equation for the probability that a rating is at or below on the rating scale:

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

To learn which of the four models described in hypotheses 2-4 characterizes the sample, comparison Chi-squared tests were performed on the ordinal regression models. Model I excludes technology-specific variables and is the technology-neutral model (the null hypothesis) in Eq. (1) above. Model I assumes that neither the base threshold privacy expectations nor the weighted importance for specific privacy factors change by technology.

Model II, based on Hypothesis 2, includes a technology factor for email and Facebook and constrains the coefficients to be the same for all locations as in Eq. (2) below:

$$\begin{aligned}\ln(P(Y \leq j)) &= \ln(Y_j) \\ &= \alpha_j + \gamma \mathbf{Email} + \delta \mathbf{Facebook} + \sum \beta X + \varepsilon_j\end{aligned} \quad (2)$$

Model III allows each technology to have different coefficients without any 'shift' in the equation—Eq. 3a illustrates technology-specific Sensitive Content variable, Eq. 3b illustrates the technology-specific Wrong to Disclose variable, and Eq. 3c illustrates the both variables with technology-specific coefficients:

$$\begin{aligned}\ln(P(Y \leq j)) = \ln(Y_j) &= \alpha_j + \beta_{1email} \mathbf{Email} \text{SensitiveContent} \\ &+ \beta_{1FB} \mathbf{FB} \text{SensitiveContent} \\ &+ \beta_2 \text{WrgDisclose} + \varepsilon_j\end{aligned} \quad (3a)$$

$$\begin{aligned}\ln(P(Y \leq j)) = \ln(Y_j) &= \alpha_j + \beta_1 \text{SensitiveContent} \\ &+ \beta_{2email} \mathbf{Email} \text{WrgDisclose} \\ &+ \beta_{2FB} \mathbf{FB} \text{WrgDisclose} + \varepsilon_j\end{aligned} \quad (3b)$$

$$\begin{aligned}\ln(P(Y \leq j)) = \ln(Y_j) &= \alpha_j + \beta_{1email} \mathbf{Email} \text{SensitiveContent} \\ &+ \beta_{1FB} \mathbf{FB} \text{SensitiveContent} \\ &+ \beta_{2email} \mathbf{Email} \text{WrgDisclose} \\ &+ \beta_{2FB} \mathbf{FB} \text{WrgDisclose} + \varepsilon_j\end{aligned} \quad (3c)$$

Finally, the privacy equation could be fully technology-specific with both a shift factor as well as technology-specific coefficients. Model IV allows all factors and variables to be unconstrained and technology-specific each with own slope and coefficients. Equation 4a illustrates both technology-factors (dummy variables) with technology-specific Sensitive Content. Equation 4b illustrates both technology-factors with technology-specific Wrong-to-Disclose content.

$$\begin{aligned}\ln(P(Y \leq j)) = \ln(Y_j) &= \alpha_j + \gamma \mathbf{Email} + \delta \mathbf{Facebook} \\ &+ \beta_{1email} \text{EmailSensitiveContent} \\ &+ \beta_{1FB} \mathbf{FB} \text{SensitiveContent} \\ &+ \beta_2 \text{WrgDisclose} + \varepsilon_j\end{aligned} \quad (4a)$$

$$\begin{aligned}\ln(P(Y \leq j)) = \ln(Y_j) &= \alpha_j + \gamma \mathbf{Email} + \delta \mathbf{Facebook} \\ &+ \beta_1 \text{SensitiveContent} \\ &+ \beta_{2email} \mathbf{Email} \text{WrgDisclose} \\ &+ \beta_{2FB} \mathbf{FB} \text{WrgDisclose} + \varepsilon_j\end{aligned} \quad (4b)$$

These models will support the examination of Hypotheses 2 with three tests of homogeneity using comparative chi-2 test. To examine an overall shift based on location, Model I is compared to Model II. To examine the statistical significance of the technology-specific coefficients, Model I (constrained) is compared to Model III (unconstrained). To examine if both the coefficients and 'shift' variables vary based on technology, Model IV is compared to Model II and Model IV is compared to Model III.

OLS respondent level equation

To examine respondent level influences, the expected privacy judgment is ordinally regressed separately for each respondent on vignette privacy factors (sensitive content, the designation wrong to disclose, etc.) thereby obtaining five parameters of the respondent-specific privacy expectation function (two thresholds, the coefficient of wrong to disclose, the coefficient of sensitive information, and the dependent variable), the corresponding standard errors, and model fit statistics (Log Likelihood, N, pseudo R-squared). This data is used to estimate gender and undergraduate effects on the shift variables as well as the coefficients in Hypothesis 3 below.

[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 2005; Kennedy, 2003) which impacts analysis below.

For the respondent level regression, if N is the number of the respondents with demographic variables (gender and undergraduate status) and K is the number of parameters estimated for each respondent, the general equation is:

$$Y_k = \beta_{0k} + \beta_{Mk}\text{Male} + \beta_{UGk}\text{CurrentUG} + \varepsilon_k \quad (5)$$

where Y_k is model parameter k, β_{0k} is a constant term for parameter k, Male is the dummy variable signifying a male respondent (1 if male), CurrentUG is the dummy variable signifying a current undergraduate respondent (1 if an undergraduate), β_{Mk} and β_{UGk} are regression coefficients for the Male and CurrentUG variables for parameter k, and ε_k is a parameter residual. The model conceptualizes the ordinal coefficients and other parameters as a function of the characteristics of the respondent.

Results

Hypothesis 1: technology gaps

Within a given conversation or information exchange, do privacy expectations change based on the technology used? **Hypothesis 1a and 1b** predict that locating the exchange across different technologies will impact the underlying distribution of the privacy expectation due to the novelty of the technology or the physical context of the technology. To test the first set of hypotheses, the mean, the cumulative probabilities, and the predicted probabilities of the privacy expectation dependent variable were calculated.

The findings support the prediction in Hypothesis 1a that privacy expectations differ when locating an information exchange across novel technologies. The results in Fig. 2 illustrate the mean privacy expectation for each location with 95 % confidence intervals. Since the dependent variable ranged from 1 (*OK to Share*) to 3 (*Wrong to Share*), the higher privacy expectation corresponds to a greater probability to find the information *Wrong to Share*. Figure 2 shows both Facebook scenarios—a Facebook Post and a Facebook Feed—as having a lower mean privacy expectation; respondents were more apt to rate information *OK to Share* on Facebook than other locations.

Figure 3 shows the cumulative proportion of responses for each location which is more traditional calculation for an ordinal response analysis. It should be noted that email has both the highest mean privacy expectation in Fig. 2 and the greatest proportion of responses rating information *Wrong to Share* in Fig. 3. As would be expected based on the context and the novelty of the technology, both Facebook locations had the highest proportion of responses with *OK to Share*. The findings provide mixed support for Hypothesis 1b that, all things being equal, locating the exchange on a platform that allows information to be easily

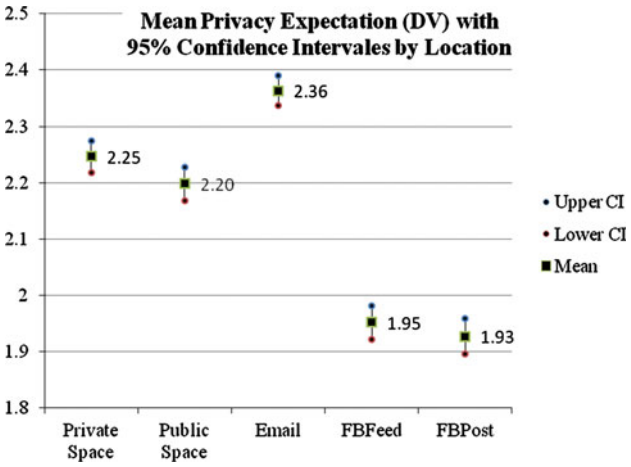


Fig. 2 Mean privacy expectation by location

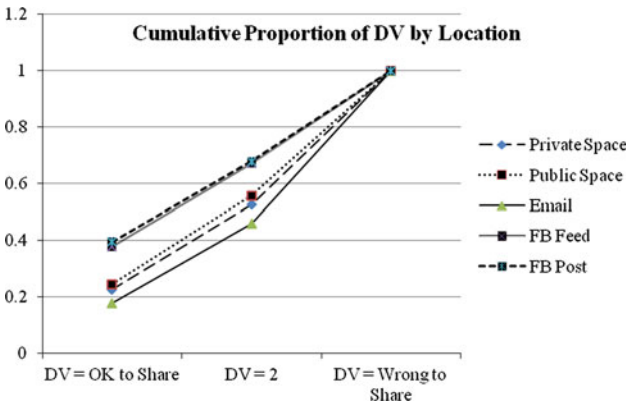


Fig. 3 Cumulative proportion of DV by location

seen or shared will decrease the privacy expectation of individuals where information would be more likely to be judged *OK to Share*. While locating the exchange on Facebook—either as a Facebook Post or as a Facebook Feed—increases the probability that the information would be expected to be shared, locating the exchange on email does not follow this trend. The cumulative probability of email emulates the distribution for a verbally exchange in a private room, thus supporting hypothesis 1a that the novelty of the technology, rather than the information friction or context, will impact the underlying distribution of the privacy expectation.

In addition, these technology gaps or differences are statistically significant. Table 1 shows the Mann–Whitney-Wilcoxon (MWW) test across locations with the MWW Z-statistic and probability for each model comparison. The MWW tests if the underlying distributions are significantly different and is a non-parametric analog to independent sample *t* test where the dependent variable need not be normally distributed and only is assumed to be ordinal. All locations have significantly different underlying

Table 1 Comparison of underlying distributions across locations

		Mann–Whitney-Wilcoxon test	
		z =	*p* =
Private space	v. Public space	−2.369	0.018
	v. Email	5.907	0
	v. FB feed	−13.306	0
	v. FB post	−14.675	0
Public space	v. Email	8.183	0
	v. FB feed	−11.317	0
	v. FB post	−12.229	0
Email	v. FB feed	−19.471	0
	v. FB post	−20.214	0
FB feed	v. FB post	−1.142	0.253

distributions aside from two cases: both (1) the difference between public and private space as well as (2) the difference between Facebook Posts and Facebook Feeds are *not statistically significant*. Verbal (private and public space) and Facebook (Feed and Post) locations are grouped together for some analysis below given they are not statistically different based on Mann–Whitney-Wilcoxon test in Table 1. This grouping provides greater statistical power in the ordinal and OLS regressions below. Also interesting in Table 1, email consistently shows greater privacy expectations in comparison to every other location—even in comparison to a private space. In fact, the largest difference in distributions is between the email and Facebook locations as evidenced in Table 1 and Fig. 2 further supporting the prediction of hypothesis 1a that information is more likely to be expected to be shared when locating an information exchange on novel technology.

Finally, Table 2 contains the predicted probabilities for each privacy expectation (1 = *OK to Share* and 3 = *Wrong to Share*) for all responses where the information in the vignette was deemed wrong to originally disclose: i.e., the proportion of responses that deemed the information both inappropriate to be originally disclosed as well as *Ok to Share*. This combination of information being inappropriate to disclose yet expected to be shared would signify the most lenient privacy norms. We would expect the predominance of the privacy expectation ratings to be *Wrong to Share* in Table 2, which it is for all locations, where information that is wrong to originally disclose should not be shared with others.

The predicted probability for being *OK to Share* given the information was deemed inappropriate to disclose within email is 0.0945. In other words, respondents rarely (9.45 %) judge information *OK to Share* if the information is deemed inappropriate for that conversation or context. Yet, for a Facebook Feed the predicted probability is 0.2249, and for a Facebook Post the predicted probability is 0.2609. In other words, the probability that information deemed inappropriate to disclose will be judged *OK to Share* with others is 2.67 times greater for a Facebook Post compared to an email. In fact, respondents *gave greater protections on email*, where the probability that information that was inappropriate to originally disclose would be wrong to subsequently share was 0.6714 (the greatest protection); and only a private room has the second highest probability that information would be judged to be *Wrong to Share* (0.6317). In sum, the results suggest statistically different distributions across locations with an increase in the probability that information deemed wrong to disclose will also be judged expected to be distributed.

Hypothesis 2–4: model comparisons

By what the mechanism are these technology differences in privacy expectations produced? **Hypothesis 2** predicts that differences in privacy expectations across technology platforms will be explained by a shift in the technology-specific base expectations. To test the second hypothesis, Chi-squared comparison tests were conducted across seven constructed models as illustrated in Table 3.

Table 2 Probability of 'anything goes' across locations: predicted probabilities for information being both *Wrong to Disclose* and *Ok to Share*

Predicted probabilities for DV (OK → Wrong to Share) if Wrg to Disclose							
	FB post	FB feed	Email	Public space	Private room	Verbal	Facebook
DV = 1 OK to Share							
OK to Share	0.5154	0.4753	0.2208	0.304	0.2816	0.2922	0.4824
Wrg to Disclose	0.2609	0.2249	0.0945	0.1169	0.1094	0.1137	0.2453
DV = 2							
OK to Share	0.2839	0.3204	0.3498	0.3838	0.3688	0.3755	0.3213
Wrg to Disclose	0.3101	0.3302	0.2341	0.2835	0.2589	0.2706	0.3428
DV = 3 Wrong to Share							
OK to Share	0.1977	0.2043	0.4294	0.3122	0.3496	0.3323	0.1963
Wrg to Disclose	0.429	0.4449	0.6714	0.5996	0.6317	0.6157	0.4119

Table 3 Comparison Chi-square across models

		Chi^2 comparison		Model fit statistics				
		Chi^2	df	LL	−2L	Chi^2	df	Pseudo R^2
Model 1: Fully constrained model				−15,002.321	30,005	2,646.6	2	0.0811
Model 2: Tech-specific base expectations								
v. model 1	0.000	697	2	−14,654.000	29,308	3,342.1	4	0.1024
Model 3a: Tech-specific sensitive content coefficient								
v. model 1	0.000	288	2	−14,858.558	29,717	2,934.1	4	0.0899
Model 3b: Tech-specific wrg-to-disclose content coefficient								
v. model 1	0.000	275	2	−14,964.697	29,729	2,921.8	4	0.0895
Model 3c: Tech-specific sensitive and wrg-to-disclose content coefficient								
v. model 1	0.000	433	5	−14,785.931	29,572	3,079.3	7	0.0943
Model 4a: Tech-specific base expectations and sensitive content coefficient								
v. model 1	0.000	704	4	−14,650.228	29,305	3,350.7	6	0.1026
v. model 2	0.023	8	2					
v. model 3a	0.000	417	2					
Model 4b: Tech-specific base expectations and wrg-to-disclose content coefficient								
v. model 1	0.000	699	4	−14,652.641	29,305	3,345.9	6	0.1025
v. model 2	0.257	3	2					
v. model 3b	0.000	424	2					

Each technology-specific models (Models II, IIIa, IIIb, and IIIc) was compared to the null hypothesis (Model I) using the Likelihood Ratio Chi Square test. The Chi Square for this between-model test is the difference between the constrained and unconstrained model Chi-Squares of the ordinal regression output in the model fit statistics with the degrees of freedom as the difference in variable between the two models. In Table 3, the statistics to the right are the individual model statistics for each model (Models I, II, IIIa, IIIb, and IIIc) and are used as inputs for model comparisons on the left hand side.

As described above, Model II added a factor for both Facebook and Email to allow for a possible shift in the privacy expectations while retaining a constraint on the coefficients of the variables in the vignette (see Eq. (2)). Model II is used to test Hypothesis 2 that differences in privacy expectations across technology platforms will be explained by a shift in the technology-specific base expectations, e.g., the Facebook Factor is 1 if the vignette is located on Facebook, 0 otherwise. The Chi-Square comparison for model II is calculated by subtracting the −2LL for the unconstrained model (Model II) from the −2LL for the constrained model (Model I) with a degree of freedom of 2. Model II is a statistically significant improvement over Model I ($\chi^2 = 697$, df $= 2$, $p = 0.000$) as illustrated in Table 3.

The same analysis is performed for each model with the results in Table 3. Each model is an improvement over Model 1, the constrained model. If the comparison χ^2 is large, we can reject the null hypothesis that the constrained model (Model 1) is correct.

Hypothesis 3 predicts that differences in privacy expectations across technology platforms will be explained by different privacy factors and their relative importance. To test the third hypothesis, the comparison χ^2 was calculated for Model IIIa versus Model I thereby examining the significance in adding a technology-specific coefficient for sensitive content. In addition, comparing Model IIIb and Model I supports examining the significance in adding a technology-specific coefficient for wrong to disclose variable. For each case, the comparison χ^2 is large and statistically significant. Both Model IIIa ($\chi^2 = 288$, df $= 2$, $p = 0.000$) and Model IIIb ($\chi^2 = 275$, df $= 2$, $p = 0.000$) are a statistically significant improvement over Model I.

Hypothesis 4 predicts that differences in privacy expectations across technology platforms will be explained by both a shift in the technology-specific base expectations as well as different weights of the privacy factors. This would be the fully technology-specific model with distinct privacy expectations as an information exchange move across technology-locations. To test the hypothesis 4, four comparisons were performed. First, the impact of adding technology-specific coefficients for sensitive content was tested by calculating the comparison χ^2 for Model IVa versus Model II ($\chi^2 = 8$, df $= 2$, $p = 0.023$); Model IVa is a *marginally* statistically significant improvement. Second, the impact of adding

Fig. 4 Model 2 ordinal regression output

```
. ologit NewDVDistrib SensitiveContent  WrgDisclose email Facebook, or

Iteration 0:   log likelihood = -16325.599
Iteration 1:   log likelihood = -14671.753
Iteration 2:   log likelihood = -14654.544
Iteration 3:   log likelihood = -14654.528
Iteration 4:   log likelihood = -14654.528

Ordered logistic regression                     Number of obs   =      15108
                                                LR chi2(4)      =    3342.14
                                                Prob > chi2     =     0.0000
Log likelihood = -14654.528                     Pseudo R2       =     0.1024
```

NewDVDistrib	Odds Ratio	Std. Err.	z	P>|z|	[95% Conf.	Interval]
SensitiveC~t	3.297409	.1114808	35.29	0.000	3.085992	3.523309
WrgDisclose	3.042774	.0997188	33.95	0.000	2.853473	3.244633
email	1.365548	.0589799	7.21	0.000	1.254707	1.486181
Facebook	.4861929	.0174053	-20.14	0.000	.4532485	.521532
/cut1	-.3637498	.0309693			-.4244485	-.3030512
/cut2	1.130866	.032389			1.067385	1.194348

technology-specific coefficients for wrong to disclose information was tested by calculating the comparison χ^2 for Model IVb versus Model II ($\chi^2 = 3$, df $= 2$, $p = 0.257$); an insignificant improvement. In other words, both technology-specific coefficients were not significant improvements. Both Model IVa and Model IVb add technology-specific coefficients to Model II without significant improvements. Therefore, Model II is preferred.

This finding was reaffirmed by two additional comparisons. The impact of adding a technology-specific 'shift' variable was tested by calculating the comparison χ^2 for Model IVa versus Model IIIa ($\chi^2 = 417$, df $= 2$, $p = 0.000$) as well as Model IVb versus Model IIIb ($\chi^2 = 424$, df $= 2$, $p = 0.000$); both comparisons illustrate a large and statistically significant improvement by adding technology-specific dummy variables—or factors—to shift the privacy expectations across technologies without changing the privacy variables and their relative importance. In sum, the findings support Hypothesis 2 that differences in privacy expectations across technology platforms will be explained by a shift in the technology-specific base expectations. In comparing the models, Model II, with both Facebook and Email factor variables, makes the largest improvement over Model I (Fig. 4).

Respondent level factors

Any differences in privacy expectations across technologies may not be uniform across individuals. For example, both undergraduate status (Young and Quan-Haase 2009) and gender (Tufekci 2008; Kuo et al. 2007) have been a factor in previous privacy studies. Therefore, we would expect both the gender and undergraduate status of the individual to impact any difference in privacy expectations across technology. To test the degree to which respondent level factors influence changes in privacy expectations, ordinal regression *for each respondent* was performed thereby building a data set with 471 ordinal regression equations for Model II, IIIa, IIIb, IIIc, IVa, and IVb. For brevity, the results of the Model II ordinal regression by respondent are shown due to the statistical significance of Model II in the analysis above. Therefore, the data set included ordinal regression output for each of the 471 respondents their model parameters including thresholds, coefficients for WrgDisclose and SensitiveContent, the technology-specific factors for Model II (b_email and b_Facebook), and model fit statistics. This data was merged with respondent demographic data on sex and undergraduate status.[8]

To identify the respondent-level factors that might influence the coefficients for the technology-specific factors (b_Facebook and b_Email) in the ordinal regression equation for each respondent, an OLS regression was performed on each coefficient by undergraduate status (CurrentUG) as well as gender (Male).[9] Overall, the mean Facebook factor (shift in the privacy expectation for being located on Facebook) is −4.96 and the mean email factor is 1.99. For the Facebook factor, current undergrads have a 3.05 greater coefficient ($p = .018$) than non-undergrads, and being male lowers the coefficient for Facebook by −2.34 ($p = .076$) as depicted in Fig. 5. For Facebook, current undergraduates are more likely to find information *Wrong to Share* due to Facebook as compared to non-undergraduates. Males are more likely to find information *OK to Share* due to Facebook as compared to females.

[8] Each respondent equation is based on between 20 and 40 rated vignettes (N = number of vignettes). Each OLS regression equation was performed using clustered and unclustered regression with no significant difference. In addition, neither the undergraduate status or gender were statistically significant determinants of the number of vignettes rated.

[9] Ideally, experience with each technology platform would also be used here, however, experience with email or Facebook was not collected in the survey. Undergraduate status may be an imprecise proxy for experience with Facebook.

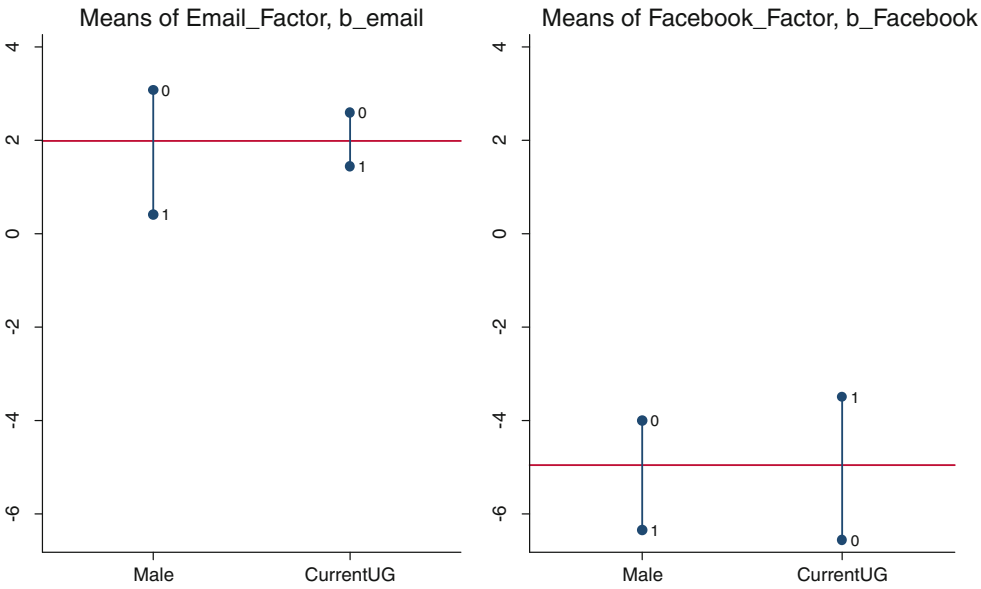


Fig. 5 Mean coefficients for Facebook and email factors from model 2

For email, males have a lower email factor than females, meaning males are more likely than females to judge information was *OK to Share* on email (male beta = −2.67, $p = .021$). In addition, current undergrad status is not a statistically significant influence for the email coefficient (beta = −1.15, $p = .313$). Therefore, while undergrads have a significantly different expectation of the role of Facebook—namely, undergrads have a 3.05 *greater* coefficient meaning undergrads were more likely to find information *Wrong to Share* (positive DV) than non undergrads within Facebook—undergrads and non-undergrads have similar expectations for the role of email in forming privacy expectations.

Discussion and conclusion

The findings of this study contribute to the literature on privacy and information technology by examining whether and how privacy expectations vary across technologies. As such, the findings speak directly to the needs of organizations to manage a diverse set of privacy issues across technology platforms.

A technology-gap in privacy expectations was *partially* supported by the findings in this study. As hypothesized, privacy expectations vary between technologies: a technology gap was found where privacy expectations significantly differ when the exchange is located on novel technology such as Facebook. Furthermore, this gap is best explained when modeled by a *shift* in privacy expectations rather than fully technology-specific privacy norms; the expectations on email and Facebook are connected to the privacy expectations offline with a different base expectation. Surprisingly, out of the five locations tested, respondents consistently assigned information on email the highest privacy protection– even greater than when locating the same exchange in a private room. In addition, while undergraduate students differ from non-undergraduates when assessing Facebook as a location, no difference is found when assessing email.

The results reported here challenge conventional views about how privacy expectations differ online versus offline. Traditionally, management scholarship examines privacy online or with a specific new technology platform in isolation and without reference to the same information exchange offline. However, in the present study, individuals appear to have a *shift* in their privacy expectations but retain similar factors and their relative importance—the privacy equation by which they form judgments—across technologies. These findings suggest that privacy scholarship should make use of existing privacy norms within contexts when analyzing and studying privacy in a new technological platform.

The results support three general conclusions. First, the privacy expectations on email have more in common with those in a private room than its technological sister, Facebook Feed. In fact, exchanges on email are offered the greatest amount of protection with the highest proportion of information deemed wrong to disclose and also judged wrong to share. This suggests that any shifts in privacy expectations may have more to do with uncertainty of a new technology rather than the technology's physical capabilities and may be *temporary*. Further supporting this conclusion, the quantile distribution graphs show less variability, and less overall uncertainty, between respondents with the less novel technology email. In addition, undergraduate students have a significantly different Facebook factor as compared to non-undergraduate students; however, undergraduate status is not a significant

factor in assessing email as a location. Once social networking becomes more integrated into the lifestyle of the respondent sample, the difference between undergraduates—who have greater experience in using Facebook—and non-undergraduates may disappear.

Second, Model II—where differences in privacy expectations are best explained by a technically-specific 'shift' factor rather than novel norms—is dominant and statistically significant throughout the analysis, thus suggesting locating an information exchange on a different technological platform has a *connection* to the privacy expectations in other locations. Finally, *privacy vacuums* are not found to be pervasive in any location as all locations had some privacy expectations and governing norms. While more information was expected to be shared if on Facebook, privacy norms still governed the location with females and undergraduate students having a statistically significant greater expectation of privacy (a greater coefficient) on Facebook.

I discuss the theoretical and practical implications of these conclusions before addressing the study's strengths and limitations.

Theoretical implications

> Why do email users perceive their communications to be private
> when email provides virtually no safe- guards against privacy violations?
> Weisband and Reinig 1995
> "Managing User Perceptions of email privacy"
> *Communications of the ACM*

As the quote above summarizes, email was considered a privacy vacuum when first adopted, and users were considered unreasonable for sharing information while retaining any privacy expectations. The findings of this study show that information exchanges on email are now regularly afforded greater normative protections by being judged *Wrong to Share*. For academics, this suggests that any conceptual muddles (Moor 1985) introduced by technology may be temporary. To work through these muddles or gaps, more research questions could be aimed at understanding *what are the privacy norms* or *how are privacy norms impacted* with a new technology rather than the more deductive *do the privacy norms match my definition*. Different privacy norms and expectations do not necessarily mean diminished or non-existent privacy expectations. Difference in privacy norms may be temporary given this study; future work on privacy could incorporate more longitudinal or time series studies to examine how privacy expectations change over time. For example, a study similar to this one could be repeated in a year or two as social networking becomes more integrated into the working and personal lives of individuals.

Second, the connection of privacy norms across technological platforms has been suggested in theory (Nissenbaum 2009). Johnson's (2004) examination of computer ethics suggests that novel technologies may introduce different act tokens of a known act type, yet "when technology changes the properties of act tokens of an act type, the moral character of the act type can change" (Johnson 2004, p. 67). These changes through a new technology have moral significance, and scholars have a role in helping individuals locate the previously developed norms and values that may provide guidance in a novel technological context. In addition, when does the change in the technological-platform modify the more general act type of human behavior? Which act type should we use as guidance in understanding a novel information exchange? This research suggests that more work could be done comparing online and offline exchanges to better understand the guiding privacy norms to look for known connections. In addition, scholars could do more interpretive work to identify when, in Johnson's words, a new technology fundamentally change the "act type" of the information exchange. Perhaps social networking sites do not introduce a temporary conceptual muddle, but a new act type with different privacy expectations. The follow-up study suggested above could empirically examine whether the expectations on Facebook converge or diverge with verbal or email exchanges. One possibility is to concentrate on the role of trust and perceived uncertainty with a new technology (Hui et al. 2007) rather than conformity to a strong conceptualization of privacy.

Finally, this study gives evidence of how an empirical examination of privacy can move away from testing the degree to which individuals agree or disagree with a strong premise of privacy by decoupling the norms of privacy (the factors and their relative importance) with the overall privacy judgment or expectation. Individuals consistently share information in uncertain environments while retaining reasonable expectations of privacy—privacy vacuums do not appear as frequently as scholarship would suggest. Again, differences in privacy norms within a particular context or with a new technology do not necessarily equate to diminished privacy expectations.

Practical implications

For organizations, the finding that new technology does not introduce completely new privacy norms, but rather a shift in privacy expectations, should provide a relief. Organizations do not need to develop new privacy norms with new technology but rather identify the connections to existing relationships and norms. As organizations continue to introduce new technologies to support existing relationships—e.g., new IT for the sales force, new features for users, introducing

Google Buzz to existing gmail customers, etc.—the findings here suggest that there will be a connection to the existing privacy expectations of the users' relationship. Therefore, the introduction of new technology or new features should be predicated by a discussion of the *existing* relationships, contexts, exchanges, and privacy expectations and how this new technology will fit.

Finally, a reliance on the privacy vacuum—or areas where 'anything goes'—where users, customers, or employees have no reasonable expectation of privacy is not supported in this study. While some locations saw a greater proportion of ratings with information both wrong to disclose and expected to be shared, all locations had norms and expectations governing the space. Organizations should ask *what are the privacy expectations of the users, customers, or employees* rather than *do users customers, or employees have any reasonable expectation of privacy here?* A reliance on the privacy vacuums may provide an excuse to not work through the difficult task of identifying the prevailing privacy expectations of stakeholders or how those expectations may change with a novel technology.

Strengths, limitations, and suggestions

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 contexts and conditions affecting judgments are systematically varied, and the highly controlled nature of the vignettes promotes greater internal validity than in usual surveys (Taylor 2006). 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. 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). In addition, 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.

Conclusion

Organizations have a vested interest in customers, employees, and users to disclose information within existing expectations of privacy. This study identified the role of technology in individuals' privacy expectations and speaks to the concerns of organizations, managers, and management scholars. While new information technology will consistently introduce new wrinkles or conceptual muddles in our privacy expectations, the findings here put these muddles into perspective by examining the same relationships and exchanges across multiple platforms.

Appendix

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.

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
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	Email	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

Question 1: Should [NAME] have shared the information with others?

Absolutely should share		OK to share	Absolutely should not share	
0	1	2	3	4

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technology*, *4258*, 36–58.

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.

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.

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.

Calo, M. (2010). People can be so fake: A new dimension to privacy and technology scholarship. *Pennsylvania State Law Review, 9*, 114.

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.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Floridi, L. (2006a). Information ethics, its nature and scope. *Computers and Society, 36*(3), 21–36.

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

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

Grimmelmann, J. (2010). Privacy as product safety. *Widener Law Journal, 19*, 793.

Hoofnagle, C. J, King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies*? (April 14, 2010). Available at SSRN: http://ssrn.com/abstract=1589864.

Hui, K., Teo, H., & Sang-Yong, T. L. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.

Hull, G., Lipford, H. R., & Latulipe, C. (2010). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology, 13*, 1–37.

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 & 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.

Johnson, D. (2004). Computer ethics. In L. Floridi (Ed.), *The Blackwell guide to the philosophy of computer and information* (pp. 65–75). Oxford, UK: Blackwell Publishers Limited.

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. G. (1982). The role of external validity in theoretical research. *Journal of Consumer Research, 10*(1), 109–111.

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.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21.

Martin, K. (2012). Diminshed or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*. doi:10.1007/s10551-012-1215-8.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, privacy and reputation (literature review). *Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10–29*. Available at SSRN: http://ssrn.com/abstract=1588163.

Moor, J. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266–275.

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

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., pp. 837–864). Bingley, UK: Emerald Group Publishing Lmtd.

O'Connell, A. A. (2005). *Logistic regression models for ordinal response variables*. Thousand Oaks, CA: Sage Publications.

Pavlou, 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.

Posner, R. A. (1981). The economics of privacy. *The American Economic Review, 71*(2), 405–409.

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

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

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.

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

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.

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.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36.

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.

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

Weisband, S. P., & Reinig, B. A. (1995). Managing user perceptions of email privacy. *Communications of the ACM, 38*(12), 40–47.

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

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of Facebook. *C&T '09 Proceedings of the fourth international conference on communities and technologies.*