BUSINESS & PROFESSIONAL ETHICS JOURNAL, VOL. 30, NOS. 1–2

TMI (Too Much Information): The Role of Friction and Familiarity in Disclosing Information

Kirsten E. Martin

ABSTRACT: Organizations have a vested interest in customers, employees, and users to disclose information within existing expectations of privacy. This empirical examination uses theoretical sampling and experimental design to identify the factors individuals consider when disclosing information within privacy expectations. The findings from a factorial vignette survey are theoretically generalizable and show that an individual's relationship to the recipient (familiarity) and the degree to which the information is protected from being easily transferred to others (friction) positively influence the odds that disclosure is judged to be within privacy expectations. The results have implications for data gathering and management of customer, user, and employee information, and suggest a two pronged strategy for organizations targeting the disclosure of information by individuals inside and outside the organization: (1) taking into consideration the familiarity of the recipient and (2) increasing the information friction of the environment.

KEY WORDS: privacy, business ethics, employee monitoring, disclosure, behavioral marketing, fair information practices.

TMI: "Too Much Information—way more than
you need/want to know about someone"
www.urbandictionary.com

 Correspondance may be sent to Kirsten Martin, The Catholic University of America, DON'T HAVE MAILING ADDRESS INFO; or via email: martin@cua.edu

Introduction

Organizations crave information. To cultivate and maintain customer relationships, firms use data mining techniques to know their customers' preferences, creditworthiness, and buying potential (Culnan and Bies 2003). Employees provide valuable productivity data to streamline operations and uncover potential problems. Teams within organizations require the free flow of information to develop new ideas and bolster creativity. Products and services—such as eBay, social networking sites, and Twitter—require more users sharing more information to be effective.

Yet, organizations need these same employees, customers, and users to have their expectations of privacy met. Privacy is positively related to the perception of trust between external stakeholders and organizations and strengthens the associated relationship with the firm (Culnan and Armstrong 1999). When employees' privacy expectations are met, organization citizenship behavior and creative performance increases (Alge, Ballinger, Tangirala, and Oakley 2006) and stress decreases (Stone and Stone 1990). Within work teams, respecting privacy is necessary for effective relationships as privacy preserves groups by providing rules of engagement and dissociation within groups (Schwartz 1968; Moore 2003). In general, privacy is instrumental to fairness and trust across stakeholder relationships (Beltramini 2003; Koehn 2003; Pollach 2005; Roman and Cuestas 2008); respecting privacy expectations entails respecting the legitimate interests of stakeholders.

The holy grail of information management for organizations would be the disclosure of information within expectations of privacy. In other words, we desire "the right of human beings to learn about one another" (Singleton 1998, 4) *as well as* the right to be left alone (Warren and Brandeis 1890). Much of the privacy scholarship mistakenly positions these interests as antagonistic with a fundamental tension between corporations and consumers (Bies 1993; Borna and Avila 1999; Sama and Shoef 2002), employee versus employer (Persson and Hansson 2003), and the general rights of individuals versus a company's business interests (Alder, Schminke, and Noel 2007; Loch, Conger, and Oz 1998; Smith, Milberg, and Burke 1996). However, organizations need both the protection of privacy interests and the disclosure of information.

Toward this end, recent focus has been on fair information practices (FIP) as a tactic to allow for the contemporaneous disclosure of information and respect of privacy norms by ensuring individuals have adequate notice and consent as to the data collection, secondary use, and data correction

(Shaw 2003; FTC 2010). The beauty of FIP is the universal nature of the guidance and the possibility of disclosing information within expectations of privacy. While definitions and applications of FIP vary, FIP has become synonymous with how we protect privacy (Bowie and Jamal 2006; Peslak 2005; FTC 2010) and is seen as successfully addressing privacy concerns (Culnan and Armstrong 1999) through adequate notice and consent.

While notice and consent are appealing in theory, FIP has been found to be neither necessary nor sufficient for privacy protections: we can meet privacy expectations without FIP and we can have FIP while violating privacy expectations (Beales and Muris 2008). FIP's limited focus on personal data and rules is widely accepted as protecting privacy, yet FIP does "not attempt to address privacy in the broader sense or to seriously limit to the collection of data" (Bonner 2007, 225). Further, restricting information can be important to prevent people from knowing about you (Alfino and Mayes 2003), to maintain a sense of self, and to leave a back space to develop personalities, goals, and ideas (Rosen 2001). The present focus on fair information practices does not account for this need to *discriminately share* information. As such, business ethics has become too focused on the actual contract of FIP and lost focus on the implicit or hypothetical contract between individuals which guides privacy norms where individuals disclose information without assuming it is 'public'—even with young adults (Hoofnagle 2010). In fact, there is *no* correlation between providing personal information online a lack of concern for privacy (Marwick, Murgia-Diaz, Palfrey 2010; Tufekci 2008); individuals regularly disclose information while retaining robust expectations of privacy. Yet, FIP offers little guidance on who and what to take into consideration in developing expectations of privacy about disclosing information.

The goal of this study is to identify the norms of disclosing information: what do individuals take into consideration when disclosing information? Finding empirical evidence of privacy norms of disclosure would suggest individuals take into consideration more than FIP when deciding when information is judged wrong to disclose. In addition, such a finding may help explain how customers, employees and users disclose information while maintaining expectations of privacy.

I leverage literature from philosophy of technology, management cognition, and privacy theory to develop hypotheses around the factors that influence privacy norms around disclosing information. I hypothesize that norms of disclosure are a function of an individual's relationship with the recipient (familiarity) and the degree to which the information is protected from being easily transferred to others (friction). Both factors have

been proposed theoretically but have not been empirically examined. I then study the model of norms of disclosure through a factorial vignette survey. This examination uses theoretical sampling and experimental design to test the concept that disclosure is based on the familiarity of the recipient and the friction of the environment. Therefore, the findings are *theoretically generalizable* and have implications for organizations who seek the disclosure of information while maintaining expectations of privacy in the data gathering and management of customer, user, and employee information. Similar to experimental studies in behavioral economics, the findings speak to extrapolating the use of familiarity and friction to understand disclosure *in general* to the world beyond (Levitt and List 2007, 153).

Theory and Hypotheses

Within this study, privacy is defined as an agreement between parties as to the allowable, expected, and inappropriate information to be shared and distributed (Nissenbaum 2004; 2009). As such, this paper is within a more contextual approach to privacy which views privacy as a negotiated set of norms about information within a specific sphere, space, relationship, or context (Brenkert 1981; Jiang 2002; Martin 2010; Nissenbaum 1997; 2004; 2009; Schonsheck 1997; Solove 2006).[1] In general, people are privacy pragmatists: individuals consider the consequences of information use and misuse and are willing to exchange information for benefits (Beales and Muris 2008). These agreements can be between friends, lovers, colleagues, or customers and an organization. Individuals act under expectations of privacy—individuals feel wronged, invaded, used, or disrespected based on our reasonable expectations of privacy norms rather than a universally-defined version of privacy.

The concept of a privacy exchange or privacy calculus is not new (e.g., Culnan and Bies 1999). However, the predominance of privacy scholarship within business ethics, and ethics more generally, has focused on norms governing secondary use or third party access of *previously* disclosed information. We focus on *active* privacy in the illegitimate collection, reproduction, or manipulation information (Floridi 2006). This focus on active privacy violations is understandable given recent technological advances facilitating the inadvertent and purposeful distribution of disclosed information. Individuals have legitimate concerns around what happens to information once in the hands of a corporation, a doctor, a manager, or a friend.

However, secondary use, or third party access, of previously disclosed information is only half of the privacy calculus, and general privacy scholarship has consistently recognized that not all information should be initially disclosed. The disclosure of information can be expected or inappropriate for a given situation and relationship (Nissenbaum 2004), and the disclosure of information of an intimate nature must be to an *interested* audience (Elgesem 1999). We retain expectations around decision and personal privacy where interference in decisions and unwanted information is deemed a breach of privacy expectations (DeGeorge 2003). And, our interest in being left alone means an interest in voluntary seclusion (Schwartz 1968; Moore 2003). Or, as philosophy of technology scholar Floridi summarizes, "Brainwashing is as much a privacy breach as mind-reading" (Floridi 2006, 111). These *passive* privacy violations occur when someone is forced to acquire unwanted information (Floridi 2006).

The question remains, what do we consider in disclosing information within an expectation of privacy? Disclosure must respect the interests of both the discloser and the recipient and the right to disclose stops "where such preferences happen to conflict with another person's claim to something" (Nissenbaum 2004, 117). Therefore, theory suggests these norms governing when information should be disclosed must include the interests of the data subject or discloser and the data recipient to respect the interests of both parties and maintain sustainable social norms. Actual or hypothetical social contracts about the accessibility of information relies upon all parties being respected, autonomous agents willing to enter such an agreement.

Toward this end, I explore two factors of any given situation that impact whether or not disclosure of information is judged to be within privacy expectations: the familiarity of the recipient and the physical context of the environment in the form of the perceived information friction. The theoretical relationships are illustrated in Figure 1.

Familiarity of the Recipient

As noted by privacy scholar Nissenbaum (2004; 2009), norms of disclosing information depend on the relationship with the recipient, and people develop different rules for friends and strangers around not only the type of information but also the burden of revelation and receipt. The disclosure of information can be mandatory, expected, voluntary, or even inappropriate within a given relationship (Nissenbaum 2004). In other words, appropriateness of information depends on the recipient of information, and the degree of familiarity between individuals impacts the amount of

information disclosed. In fact, there is some information that is not appropriate or even damaging to disclose. As noted by Schoeman (1984), "revelation of self is not to be thought of as desirable in itself and may be detrimental." In common parlance, we declare TMI or 'too much information' to signal when someone is disclosing too much for the given relationship.

The type of relationship between individuals influences disclosure because, all things being equal, people tell more to those they know and less to people who are unfamiliar. Individuals restrict information because it prevents others from knowing about them (Alfino and Mayes 2003) and withhold information to avoid being "misrepresented and judged out of context" (Rosen 2001, 21). For strangers with little familiarity and without an established relationship, restricting disclosure is particularly important as individuals rely upon intuitions in assessing new situations or people (Dane and Pratt 2007). Individuals process information that fits their expectations and find reasons to exclude the information that might contradict it (Perrow 1999). In other words, people make snap judgments about new individuals. In fact, individuals can elaborate and embellish based on single points of reference or extracted cues, and these initial impressions require work to re-orient (Weick 1995).[2]

Therefore, familiar relationships with trusted individuals are prepared for more information to be disclosed. Not only is privacy necessary for intimacy (Elgesem 1999) by according people the important power to share information discriminately across relationships (Nissenbaum 2004; Rachels 1975), but *discriminately sharing* information is also a symbol of the strength of a relationship (Fried 1984) and a necessary measure to protect a new relationship.

> ***Hypothesis 1a****. Individuals will be more likely to judge the disclosure of information to be within privacy expectations in relationships with greater familiarity as compared to strangers.*

In addition, the level of transparency is not all or nothing, but 'optimal' depending upon the type of information and the maturity of relationship (Brin 1998). Individuals grant different people different levels of access at different times (Moor 1997). Therefore, privacy is not violated by the mere act that information is known, but is contingent on the relationship between the discloser and the recipient (Brenkert 1981).

Information that is expected within one relationship becomes inappropriate in others. Information shared between spouses is not necessarily shared at work, and information disclosed to a business is not necessarily

to be disclosed to friends.[3] As such, the flow of information is not the same for everyone. The norms of disclosure about *specific* types of information are a function of the level of familiarity between the data subject and data recipient (Nissenbaum 2004). Therefore, the degree of closeness or familiarity will influence not only the quantity of information disclosed but also the particular norms around disclosing specific information.

> ***Hypothesis 1b.*** *Individuals have different norms of disclosing particular information for strangers as compared to friends/colleagues.*

Information Friction

In addition to the relationship between parties, the norms of disclosure must also consider the future risks to the data subject more generally and not merely the immediate relationship. How vulnerable is the information? How easily transmitted or *greased* is the information (Moor 1997)? The context of the situation—what Floridi (2000, 2006) calls information friction—can impede the future transmission of the information thus rendering the information 'safe.'

Information friction are the forces that oppose information flow within a given situation (Floridi 2006b) and influence the amount of work necessary for individuals to obtain information about others. As Floridi illustrates, walls offer more friction and greater privacy protection than thin partitions in hospitals. However, friction need not be as material as walls: distance, noise, lack of resources (memory/time), amount and complexity of information all contribute to information friction as perceived by the individual (Floridi 2006a). Talking in a large public space may offer more information friction than when in a small room with few people. Legal scholar Jeffrey Rosen (2001) gives an example of an old fashioned pharmacy in Georgetown that is successful due to a policy of dispensing all prescriptions by hand and not keeping computer records. These handwritten records afford greater friction to the future accessibility and transmission of the data for the customers. The amount of friction perceived by the discloser of information as friction lessens the risk of unwanted use, access, and distribution of information. Privacy, according to Floridi, is a function of friction.

More importantly, perceived friction—in the form of technology, architecture, and material structures—offers individuals the comfort to be able to share information with an expectation the information will be contained or slowed down. If it is believed that information will not flow freely due to the friction of the situation, individuals will be more likely

to believe disclosure of information is safe. Similar to the hand written records in the case of a pharmacy in Georgetown (Rosen 2001), friction is found in the physical architecture and the social norms of the context, impedes future information flow, and supports the disclosure of information within and expectation of privacy.

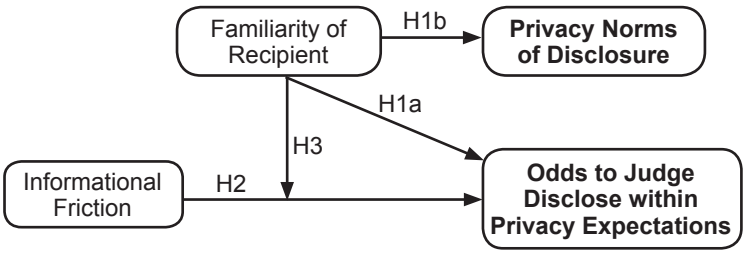
> ***Hypothesis 2***. *All things being equal, individuals will be more likely to judge disclosure of information to be within privacy expectations in contexts with greater information friction.*

While Floridi uses the concept of information friction, the general idea that specific constraints and affordances oppose and facilitate information flow is found in theory throughout privacy scholarship. As Moor (1990) notes, we can be in both naturally private situations based on physical barriers and normatively private situations based on context and relationships. Similarly, Lessig (1998) focuses on the use of architecture as well as social norms to protect information, and Reiman (1995) notes that we protect information through both material structures and formal rules where privacy results not only from locked doors and closed curtains, but also from the way our information is dispersed over space and time.

Therefore, familiarity influences disclosure due to the maturity of the relationship as identified in Hypothesis 1. In addition, familiar relationships have the opportunity to develop strong norms around the flow of information.[4] These social norms govern the appropriate exchange of information and form an alternative form of friction. While friction works through both material architecture and social norms to increase privacy, both avenues may not be necessary for individuals to share information within an expectation of privacy and "in human societies, privacy is also fostered through tacit agreements" (Floridi 2006b, 117). "Norms of decency, etiquette, sociability, convention, and morality frequently address appropriateness and distribution of information" (Nissenbaum 2004, 157). Therefore, in the presence of strong social norms, physical friction may not be as necessary. The greater the familiarity between parties, the greater the influence of social norms about privacy and the less information friction should be a factor in rendering it more likely find disclosure of information within privacy expectations. Within an unfamiliar relationship, friction is a greater factor in maintaining an expectation of privacy.

> ***Hypothesis 3***. *Physical friction will be a larger factor for strangers as compared to colleagues in judging the disclosure of information to be within privacy expectations.*

Figure 1: Factors Influencing Privacy Norms of Disclosure



Methods

The objective of this study was to identify the factors that contribute to an expectation that information should or should not be disclosed. This is a proof-of-concept examination—a theoretical examination (Lynch, 1983)—therefore the findings will support or not support the theoretical suggestion that individuals take into account the familiarity of the recipient and the friction of the environment when disclosing information and extrapolating the findings to the world beyond. Such research seeks the generalizability of ideas rather than the generalizability of data patterns within a specific population (Lynch, 1983). The findings speak to extrapolating the use of familiarity and friction to understand disclosure *in general* to the world beyond (Levitt and List 2007, 153).

I used factorial vignette methodology developed to investigate human judgments (Rossi and Nock 1982; Jasso 2003). In a factorial vignette survey, respondents are asked to evaluate a set of vignettes, where the vignette factors or independent variables are randomly selected by the researcher. The methodology allows for the simultaneous experimental manipulation of a large number of factors through the use of a contextualized vignette (Ganong and Coleman 2006).

Factorial vignette survey methodology is designed to identify normative judgments which are dependent on contextual factors and 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). The approach, therefore, is particularly well suited to the examination of privacy norms of disclosure as the exact factors are not established and norms may vary based on changes in the context of the vignettes as well as different subgroups of the respondents.

Theoretical research, as compared to effects application research, investigates relationships among ideas or constructs (Lynch 1983). 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 1983, 233). Here, I am representatively sampling factors in order to test the conceptual model in Figure 1.

A set of vignettes was generated for each respondent which described a hypothetical situation wherein a protagonist disclosed information in a particular context. The context varied based on the type of information, the familiarity of the recipient to the protagonist, and the informational friction of the situation (see Appendix A for an example); these factors or explanatory variables are explained below. After construction, unrealistic scenarios and combinations were removed and the instrument was pilot tested.

Explanatory Variables

The primary explanatory variables in this study are the factors that constitute the vignettes. The number and levels of vignette 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).

Type of Information. According to Hypotheses 1b, individuals have different norms of disclosing particular information for strangers as compared to friends/colleagues. The type of information willingly disclosed should differ based on the familiarity of the recipient. These norms are operationalized as the different expectations around the *type* of information shared (Nissenbaum 2004; Brenkert 1981). Therefore, five types of information were systematically varied in the vignettes from public information to very private information to examine if, at all, individuals assign different levels of importance to varying content across familiarity.

Familiarity of Recipient. The theoretical model described above, and depicted in Figure 1, relies upon individuals having different privacy norms and expectations based on the degree of familiarity. Familiarity is important for two reasons: (1) the amount of time individuals know each other allows individuals to put disclosed information into perspective (Hypothesis 1a) and (2) familiar individuals have developed privacy norms to govern rules of information exchange rather than information friction only (Hypothesis 3). To operationalize familiarity, I chose two

theoretically extreme situations to clearly distinguish between familiar and unfamiliar individuals: the recipient was either a fellow member of an ill-defined group of strangers or a well-defined team in the form of an athletic team. Athletic teams have been compared business teams previously (Katz and Koenig 2001; Wolfe et al. 2005): they are similar in structure and motivation and, importantly for this study, membership and stability are important. Athletic teams are considered a living laboratory (Keidel 1987) conducive to isolating factors important to leadership and group dynamics similar to other extreme team activities such as combat units, astronaut work units, and surgical teams (Adler and Adler 1988).

College athletic teams, in comparison to ill-defined group of strangers, operationalize the two important factors of familiarity. First, athletic teams have longer relationships than ill-defined assigned teams by definition—the individuals have known each other and will work together towards a common goal in the future. Participants spend more time together and have a willingness to forgive each other (Keidel 1987). Second, athletic teams are intensely loyal (Alder and Alder 1988) and have extreme sensitivity to the insider-outsider distinction (Jonassohn, Turowetz, Gruneau 1981). In fact, management scholars have found college athletic teams to be "structured so that individuals are dependent on the success of the group for their own success" (Adler and Adler 1988). Athletic teams are well defined, goal-oriented, *norm-generating* communities of individuals who have the opportunity and need to develop privacy norms which is needed to test the hypotheses. Therefore, in order to identify changes in privacy expectations across different recipients, the data was analyzed based on the recipient as a stranger versus a colleague and this difference in familiarity is theoretically generalizable to relationships within organizations and relationship between organizations and stakeholders.

Information Friction. Two factors were combined to produce the degree of information friction of the scenario. First, the physical context varied between verbal communication, email, and social networking site in *decreasing* informational friction. As noted by Moor (1997), our information becomes increasingly greased and easily transferred as we move from verbal communications to the use of information technology. Social networking would be a further extension of the trend as communication is not easily controlled or targeted.

In addition, the information friction of a situation is not necessarily objectively known by all parties. The degree to which the protagonist intended to share information and understood the information friction of the situation would be an additional consideration adding to the friction due

to the physical context. Knowledge about how information is accessible within a particular context is important for privacy expectations (Schonsheck 1997). Therefore, to test the impact of information which is unintentionally versus intentionally shared, vignettes varied if the information was unintentionally shared by being overheard or intentionally disclosed by being the recipient prodding the information from the protagonist. In the case of the former, the informational friction would be increased as the protagonist of the scenario believed himself to be in a situation within higher information friction. In the case of the latter, the informational friction would be decreased as the protagonist of the scenario understood the recipients and the context clearly. Combining these two factors, the perceived information friction could vary on a five item scale. As this is a contrived measure of friction for the concept's theoretical role in disclosing information, the analysis below merely compares *low* and *high* friction environments.

Sample

I tested the model and hypotheses with 15,736 observations from a larger privacy study examining privacy as a social contract (xxxx 2010) with 19,737 total observations. The original sample was recruited via e-mail within a single institution with heads of departments and teams as the primary contacts who forwarded the survey to their members. Of the original 937 respondents, *undergraduate students comprised only 50.6% of the sample*; and females comprised 53.8% of the sample thus allowing the analysis to control for undergraduate status and sex. The unit of analysis in this research is the rating of a vignette (N = 15,736).

Dependent Variable

Respondents were asked to judge the named protagonist in the story who disclosed information to either a stranger or a colleague. After each vignette, the same question was asked of the respondent "Should the teammate have initially disclosed the information?" 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 Tell*) to 4 (*Wrong to Tell*) (Nissenbaum 2004) to signify the degree to which disclosing information was within or outside privacy expectations. However, during analysis the first three ratings were combined and recoded to form a three rating scale during analysis due to the small number of ratings of 0 or 1. Therefore, the analysis below is based on a three item ordinal rating from 1 (*OK to Tell*) to 3 (*Wrong to Tell*).

Analysis

The data in this study was in two levels: the vignette level factors and the respondent level control variables. For the larger survey, 937 respondents rated a range of 0–40 vignettes resulting in 21,187 rated vignettes or total observations. However, the data analyzed here consists of 15,736 of the total observations due to the theoretical focus in examining friction and familiarity. 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:

$$(1)\ \ln(P(Y_{nk} \leq j)) = \ln(Y_{nk}) = \alpha_j + \Sigma\beta_i V_{ik} + \Sigma\gamma_h R_{hn} + u_n + e_k$$

where Y_{nk} is the rating of vignette k by respondent n, V_{ik} is the i^{th} factor of vignette k, R_{hn} is the h^{th} characteristic of respondent n, is the threshold term for level j, β_i 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.

In testing the hypotheses, I used ordinal regression 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.[5] Strong associations between explanatory variables and ratings are represented by coefficients farther away from 0.0 and odds ratios farther away from 1.0 (since OR = exp(β)). A positive coefficient would have an odds ratio greater than one and would signify the associated explanatory variable would have an upward impact on the rating task.[6]

For factorial vignette surveys, the number of vignettes is typically set at 10–60 vignettes for each respondent to answer. However, this 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 issue of respondent fatigue or respondent burden within factorial vignette surveys (Nock and Gutterbock 2010): i.e., when the judgments *and associated errors* cannot be assumed to be independent due to correlation within a single respondents' answers, whereas typically vignettes are pooled as independent. While respondent fatigue was a factor for some models,[7] 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 were discarded for all respondents (sequence numbers 1 and

2), the model fit criteria and parallel lines significance improved dramatically. I discarded all vignette ratings with a sequence number of 1 or 2 for the entire analysis.

In running the ordinal regression, I examined the significance of the explanatory variables, the model-fit criteria, and the parallel-lines assumption. All potential explanatory variables were included in the initial regression analysis and subsequently excluded if found to be insignificant in the ordinal regression. Reduced models were run both with the logit link and the complementary log-log (cloglog) link based on the distribution of ordinal outcome, either evenly distributed among all categories or clustered around lower categories. Finally, the best model was chosen among all candidate models based on the model fitting statistics, the validity of the parallel-lines assumption, and the principle of parsimony.[8]

It should be noted that while "it has become cliché to claim that young people don't care about privacy, studies have shown young people are in harmony with older Americans when it comes to privacy attitudes (Hoofnagle 2010, 20). This study further supports the congruence of privacy attitudes between younger and older adults since undergraduate status is almost insignificant ($\beta = .010$) when controlled for in regression analysis.

Results

Hypothesis 1a predicts *individuals will be more likely to judge disclosure of information to be within privacy expectations for colleagues as compared to strangers*. To test hypothesis 1a, I divided the data into scenarios based on the familiarity between parties (colleagues versus strangers) and compared both the cumulative probability that the judgment that the disclosed information was within privacy expectations as well as the mean dependent variable for each group.[9] When in a scenario with colleagues, individuals judged the disclosure of *any* information to be within privacy expectations 56.3% as compared to 54.0% when in a situation with strangers. Individuals on average were more likely to judge information *Wrong to Tell* when presented with a scenario with strangers (mean = 1.637) as compared to colleagues (mean = 1.596, Mann-Whitney $Z = –3.271$, $p = .001$). The findings support the prediction in hypothesis 1a that individuals will be more likely to judge information is *OK to Tell* for those familiar to them as opposed to strangers.

Hypothesis 1b predicts *individuals will have different norms of disclosure for strangers as compared to colleagues.* To test hypothesis 1b, I

performed ordinal regression analysis for both colleagues and strangers as depicted in Table 1. Table 1 shows the effects of the vignette factors as independent variables on the dependent variable with both significant standard βs and odds ratios (OR) provided to illustrate the relative importance of the vignette factors on the rating task. For example, while the content of information is consistently associated with higher categories on the privacy rating, the amount of influence varies based on the familiarity of the recipient. The use of odds ratios permits the comparison of factors and their importance across models: we can say, all things being equal, vignettes with private content *raise the odds* of finding information *Wrong to Tell* by 2.8 times for colleagues in model 1 as compared to vignettes without private information.

Table 1: Ordinal Regression Results By Familiarity

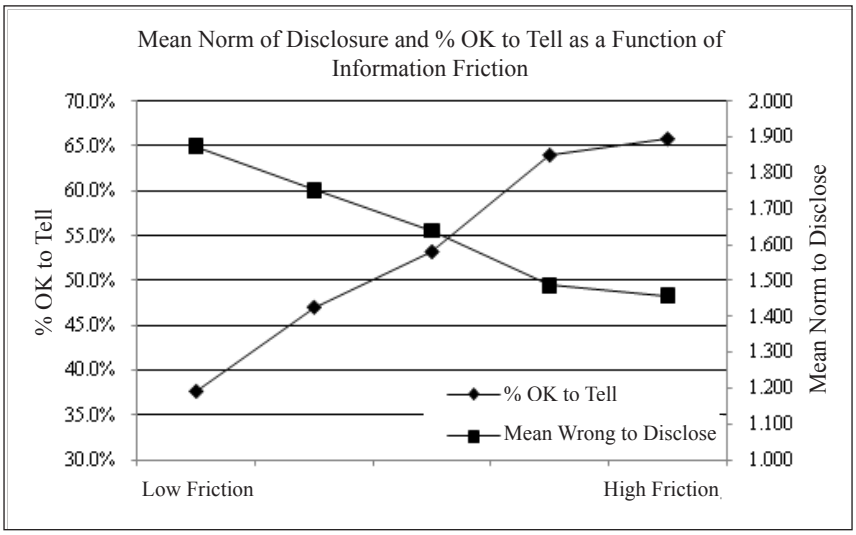
Ordinal Regression Results				
	Colleagues		*Strangers*	
mean =	1.59		1.64	
n =	8127		7590	
	Model 1		*Model 2*	
	β*	OR**	β	OR
Content				
role based	0.686	2.0	0.674	2.0
personal	0.808	2.2	0.915	2.5
family	0.473	1.6	0.930	2.5
private	1.041	2.8	1.509	4.5
High Friction	–0.396	0.7	–0.460	0.6
Control Variables				
Male	0.084	1.1		
Undergrad	–0.090	0.9		

** All coefficients shown with significance < .01*

*** Odds Ratio = OR = exp(β)*

Models 1 and 2 in Table 1 illustrate the different norms for disclosing information for strangers and colleagues. Perhaps most strikingly, the type of information is consistently a larger factor for strangers as compared to colleagues with private information 4.5 times as likely to be more *Wrong to Tell* with strangers as compared to colleagues where respondents are only 2.8 times as likely to find private information *Wrong to Tell*. Colleagues appear to have a more generic 'tell/don't tell' policy whereas strangers have a more nuanced set of norms with different factors impacting the judgment that the disclosure of information is within privacy expectations. In other words, the specific type of content is less of a factor for colleagues. The findings support the prediction in hypothesis 1b that norms of disclosure will vary based on the degree of familiarity of the recipient. Models 1 and 2 illustrate that individuals have different disclosure norms for strangers and colleagues as evidenced by the different factors and coefficients the respondents took into consideration when assessing particular information was *Wrong to Tell*.

Figure 2: Privacy Expectations as a Function of Information Friction



Hypothesis 2 predicts *individuals will be more likely to say the disclosure of information is within privacy expectations for scenarios with greater physical information friction.* To test hypothesis 2, I compared both the mean dependent variable as well as the cumulative proportion

that the judgment that the disclosed information was within privacy expectations. Specifically, the cumulative proportion of ratings deemed to be within privacy expectations increased from 37.6% to 65.8% in low friction and high friction scenarios respectively. This trend is illustrated in Figure 2. For high friction scenarios, the disclosure of information was more likely to be judged within privacy expectations and considered *OK to Tell* (mean = 1.477, Mann-Whitney Z = –18.812, p = .000) compared to low friction scenarios, where the disclosure of information was deemed more *Wrong to Tell* (mean = 1.790, Mann-Whitney Z = –17.423, p = .000) as illustrated in Figure 2. The findings support the prediction in hypothesis 2 that individuals were more likely to judge the disclosure of information to be within privacy expectations for scenarios with greater friction.

Hypothesis 3 predicts physical friction will be a larger factor for strangers as compared to colleagues. To test hypothesis 3, I compared the impact of friction on both the mean disclosure norm as well as the cumulative proportion of judgments that information was within privacy expectations by calculating the cumulative proportion and mean for each level of friction for both strangers and colleagues. I found an increase in friction decreased the mean disclosure norm for both strangers (from 1.790 to 1.393, Mann-Whitney Z = –9.935, p = 0.000) and colleagues (from 1.888 to 1.501, Mann-Whitney Z = –15.979, p = 0.000). The relationship persists regardless of the familiarity of the relationship with greater friction correlated with a greater proportion of judgments being rated within privacy expectations regardless of the type of information shared. In comparing the impact of friction in both levels of familiarity, the influence of friction on the cumulative proportion of judgments that information was within privacy expectations *appears* direct and linear for strangers—more friction correlates with a greater probability that information will be more likely to be judged *OK to Tell*. However, when disclosing information with colleagues, the relationship is positive but not quite as clear as illustrated in Figure 3.

Two additional tests for the interaction effect were conducted. First, I included a dummy variable—high friction—to identify the importance of friction as a factor in the ordinal regression equations for familiar and unfamiliar recipients as illustrated in Table 1. Friction has a similar impact for both levels of familiarity as well as across the control variables of sex and undergraduate status. Second, I added an interaction term capturing the interaction between Familiarity and HighFriction within a generalized linear regression (due to the ordinal dependent variable). The interaction term was significant (Wald = 442.350, d.f. = 4, p = .000). However, Table 2 illustrates the more specific interactions combining all possible combinations

of friction and familiarity. The results show that friction dominates relative importance of factors whereas changing the familiarity is barely significant.

Table 2: Significance of the Interaction between Friction and Familiarity

Significance of Interaction Terms using Generalized Linear Regression Analysis		Friction	
		High	Low
Familiarity	High	Null	β= 0.631 p = 0.000
	Low	β= 0.111 p = 0.079	β= 0.743 p = 0.000

Therefore, for colleagues, physical friction was *slightly* less of a factor, however given the theoretical nature of the concept 'information friction,' such a difference cannot be generalized. Therefore, while the graph in Figure 4 illustrates less of an impact of friction on the judgment information is *OK to Tell* with a slightly shallower slope for the trend line for colleagues, the relative change in slope is not conclusive. Friction appears to have a greater and more consistent impact in making the disclosure of information within privacy expectations for recipients with less familiarity to the data subject. However, the findings were *inconclusive* as to the prediction in Hypothesis 3 that an increase in informational friction will have a greater impact for strangers as compared to colleagues.

Figure 3: Cumulative Probability Information Within Privacy Expectations as a Function of Friction And Familiarity

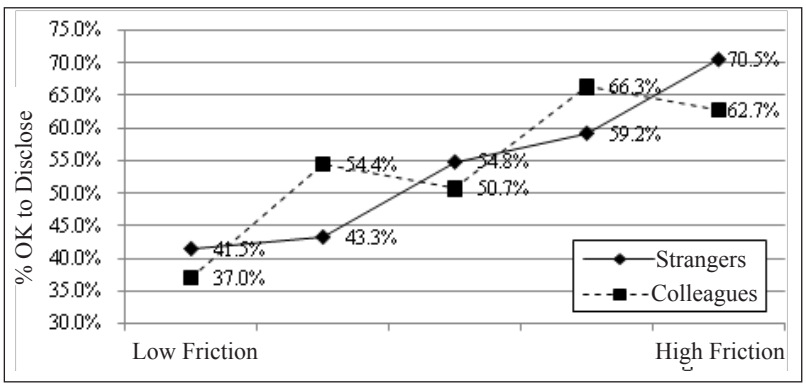
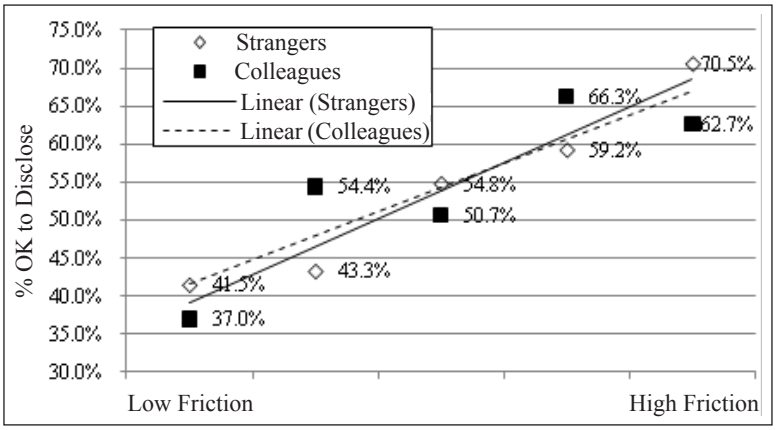


Figure 4: Familiarity as Moderating Impact of Friction on Privacy Expectations



Discussion

This study identified both the familiarity of the recipient and the information friction of the situation as important factors impacting when disclosure is judged to be within privacy norms. In general relationships matter, and individuals are more likely to find the disclosure of information to be within privacy expectations within established relationships as opposed to strangers. Furthermore, additional information friction has a direct impact on the probability the disclosure of information—any information—will be deemed within privacy expectations. However, contrary to predictions, the results did not find the existence of social norms within familiar relationships to dampen the impact of physical friction conclusively. While strong norms may moderate the importance of information friction, additional testing would be needed.

Finding empirical evidence of norms of disclosure suggests individuals take into consideration more than fair information practices when judging information is *Wrong to Tell*. As such, the study offers an alternative view of disclosure norms that more explicitly takes into account the interests of both the subject and recipient of information, the potential for a hypothetical contract around norms (Nissenbaum 2004), and a move away from relying upon rules and procedures within FIP which have become devoid of moral prescription and reflection (Bonner 2007).

More importantly, these findings may help explain how customers, employees and users disclose information while maintaining expectations

of privacy. The findings suggest that the amount of disclosure is an open conversation, and more research is needed around what to consider in deciding to disclose and receive information at the level of the organization and individual. The results suggest a two pronged strategy for organizations targeting the disclosure of information by individuals inside and outside the organization: (1) taking into consideration the familiarity of the recipient and (2) increasing the information friction of the environment. After examining the study's strengths and limitations, I discuss both factors below in addition to the implications to the study of fairness and privacy.

Study Strengths and Limitations

Factorial vignette surveys offer a unique methodology to ascertain human judgments where the survey respondent may be unable or unwilling to articulate the reasons behind their response (Wallander 2009; Taylor 2006). Participants are not asked directly why the information is judged to be within privacy expectations, but allowed to pass judgment on a randomly selected set of factors whereby the researcher can inductively identify to the factors and their relative importance for subgroups of respondents. As such, the methodology uniquely suits the topic of applied ethics in general and privacy in particular as respondent bias is mitigated, plus the concept of privacy is not easily defined or universally understood. In other words, the study supports theoretical research rather than the examination of specific data patterns within a particular subpopulation (Lynch 1983).

However, given the quasi-experimental methodology employed (Wallander 2009), the results should be generalized to theoretical trends rather than definitive prescriptions. The use of ordinal regression further supports such theoretical generalizations as we are able to state, at most, that a factor makes a judgment more likely (or less likely) to be at a higher rating. For more definitive prescriptions, additional empirical research would be needed.

Operationalizing norms and strong relationships is difficult. Here I used theoretically extreme situations by comparing a defined team and a group of strangers. Additional research would be needed to identify the change in privacy norms for subtle changes in group familiarity. In addition, this study examined one type of information friction; additional research could examine additional ways in which the information friction can vary. Floridi (2006a) offers great detail on the manner in which friction can vary across contexts. Finally, the respondents stated their judgment about the hypothetical situations rather than capture actual behavior.

Additional research could examine actual disclosure rates and ask respondents if disclosure was within expectations.

Familiarity

This study found the degree of familiarity between the data subject and recipient had a positive impact on the odds that disclosure of information is judged to be within privacy norms. This phenomenon has two possible explanations in theory: as alleviating the concerns of either the data subject or the concerns of the recipient.

First, discriminately sharing information allows the data subject to maintain her identity (Goffman 1978), a degree of disassociation (Moore 2003), and space to develop a persona (Brin 1998) by not revealing information. *Discriminately sharing* information—or limiting the amount of information disclosed—prevents individuals from being misrepresented or judged out of context. (Rosen 2001). It is important for organizations to manage the amount of information asked of employees, customer, and users and not rely upon notice and consent as adequate measures to ensure privacy is respects. Even with notice and consent, there is information that requires an established relationship before disclosure, as disclosure is instrumental to and a natural outcome of a stronger, more familiar relationship. Organizations would be better served asking additional information from more established customers and employees where the relationship is more familiar to both parties. Asking the same information from new and familiar customers or employees could elicit different responses.

In addition, the recipient of information may also be a consideration. For example, Lehavot (2009) examines whether graduate admissions officials should search MySpace for information on potential students. In doing so, Lehavot addresses a much neglected area of privacy scholarship—the need to *discriminately know* information. Individuals need to discriminately know information for good reason as more information does not equal better decisions and information taken out of context can be misleading. The use of heuristics or rules of thumb are subconscious (Tversky and Kahneman 1974) and decision makers use only part of the information that is potentially available due to cognitive limitations as well as time and resource constraints (Simon 1945; March and Simon 1958). As noted by Weick, "The problem in ambiguity is not that the real world is imperfectly understood and that more information will remedy that. The problem is that information may not resolve misunderstandings" (1995, 92). Therefore, embedding information in a particular context is necessary to give it meaning. If the recipient does not understand the context or could

improperly apply or use the information, they are not in a position to receive the information.

As Floridi (2006b) notes, everyone has an interest to know some information as well as a duty to ignore other pieces of information. Organizations managing applicant, customer, or employee information should identify limitations to what the firm needs to know and what information is unethical or impractical to receive. There is information that organizations should not know because it may bias future decisions or is too costly or risky to maintain. Taking into account the degree of familiarity protects both the data subject in *discriminately sharing* information and the recipient in *discriminately knowing* information. Future examinations should focus on the responsibility of organizations and managers to discriminately know information about customers, employees, and users. Little work has been done to examine the responsibility of knowing information and when organizations and individuals should possibly ignore information.

Friction

Within this study, perceived information friction in the form of the physical and technical context impacted the odds that disclosure would be found within privacy expectations. In practice, friction can be reduced or increased with information and communication technologies (Floridi 2005). Changing the technological capabilities and default values directly impacts the friction of the environment and, therefore, changes the context of the agreement in which the information was disclosed. As it happens, such changes rarely increase the information friction. Recent cases such as Facebook's Beacon advertising technology and Google Buzz have only served to decrease friction and increase the public's concern; both technology introductions took existing information—buying habits of Facebook users and email addresses of gmail users—and disclosed the information to other users. Organizational responses to the original user backlash centered on reiterating the actual notice and consent given to users. However even with notice and consent, users have legitimate claims as their privacy expectations were predicated on the information friction of the situation at the time of disclosure. Organizations should be aware that changing the information friction directly impacts the norms of privacy and more proactively managing the privacy implications of such modifications.

Finally, physical information friction may work up to a point. As noted by Reiman, "if we direct our privacy protection efforts at reinforcing our doors and curtains, we may miss the way in which modern means

of information collection threaten our privacy by gathering up the pieces of our public lives and making them visible from a single point" (1995, 29). It is important for organizations to examine the vulnerability of their data and communicate their protections—or their designed information friction—to employees, customers, and users. Since the perceived information friction influences the odds of finding disclosure to be within privacy norms, an independent organization who can verify the safety of the data, such as an auditing firm, may help with communicating the information friction to stakeholders.

As an astute student noted in a discussion on Facebook and privacy, "If they can make your information private that quickly, they can just as easily make it not private." We rely upon trusted institutions and individuals to keep the information private or keep the doors shut. Development of greater social norms concerning privacy—those hypothetical social contracts governing information exchange—may impact disclosure more than stronger brick walls. More focus on hypothetical social contracts or normative agreements between parties—and less on the actual notice and consent statements—would help strengthen the social norms about privacy between organizations, employees, customers, and users.

Appendix A: Sample Vignettes

(Factors are underlined)

	Attributes		Dimensions	Operationalized
1	Familiarity	0	Close Colleagues	*On a varsity athletic team*
		1	Strangers	*On an assigned project team for a required class*
2	Intention	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	Physical Friction	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*

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.*

Endnotes

1. Within privacy scholarship, two definitions dominate the scope debate: (a) private information defined as that which is *inaccessible* to others versus (b) private information defined as that which is *controlled* by an individual (Westin 1967). Both propose privacy to be static and universally applicable. See also Moor 2006.

2. An alternative view would position strangers as a safe haven where individuals are more apt to tell more to an unfamiliar individual on a place than to an acquaintance. However, the majority of privacy scholarship posits the familiarity of the relationship as positively correlated with disclosure of information.

3. For example, Facebook's Beacon program tracked a Facebook user's browsing and buying activities on commercial websites, such as Amazon.com, and sent a notice to all the user's friends. After a public backlash, Facebook modified the program (Martin 2010). Information disclosed to Amazon.com was not necessarily to be disclosed to friends.

4. It is also possible to have strong privacy norms *without* familiarity. A priest, doctor, therapist, or lawyer have strong, even regulated, norms of privacy without any familiarity of the relationship. Herein, the study attempts to parse the two different influences of *familiarity* on disclosure. Subsequent research could examine privacy norms within such

well-defined privacy norms without familiarity. I wish to thank an anonymous reviewer for pointing this out.

5. 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.

6. A few additional points differentiate ordinal regression analysis. First, a link function describes the effect of the explanatory variables on an ordered dependent variable in order to not assume either normality or constant variance (Chen and Hughes 2004). In addition, ordinal regression requires the relationship between independent variables and the dependent variable to be independent of the category—in other words, the regression coefficient does not vary based on the category of the ordinal response variable. Therefore, the assumption of 'parallel lines' was consistently verified during the analysis.

7. 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.

8. Parsimony requires models with fewer explanatory variables to be prioritized over larger models that include, by definition, insignificant variables.

9. The mean dependent variable is less meaningful for ranked dependent variables as the absolute value of each category is not necessarily consistent across respondents. Ordinal regression solves this problem by providing the degree to which a factor raises or lowers the odds that an answer would be in a higher (or lower) category.

References

Adler, Patricia A., and Peter Adler. 1988. "Intense Loyalty in Organizations: A Case Study of College Athletics." *Administrative Science Quarterly* 33: 401–417.

Alder, G. Stoney, Marshall Schminke, and Terry W. Noel. 2007. "The Impact of Individual Ethics on Reactions to Potentially Invasive HR Practices." *Journal of Business Ethics* 75: 201–214.

Alfino, Mark, and G. Randolph Mayes. 2003. "Reconstructing the Right to Privacy." *Social Theory and Practice* 29(1): 1–18.

Alge, Bradley J. 2001. "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice." *Journal of Applied Psychology* 86: 797–804.

Alge, Bradley J., Gary A. Ballinger, Subrahmaniam Tangirala, and James L. Oakley. 2006. "Information Privacy in Organizations: Empowering Creative and Extra-Role Performance." *Journal of Applied Psychology* 91(1): 221–232.

Ashworth, Laurence, and Clinton Free. 2006. "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns." *Journal of Business Ethics* 67(2): 107–123.

Beales Howard J., and Timothy J. Muris. 2008. "Choice or Consequences: Protecting Privacy in Commercial Information." *The University of Chicago Law Review* 75(1): 109–135.

Beltramini, Richard F. 2003. "Advertising Ethics: The Ultimate Oxymoron." *Journal of Business Ethics* 48(3): 215–216.

Bies, Robert J. 1993. "Privacy and Procedural Justice in Organizations." *Social Justice Research* 6: 69–86.

Bonner, William. 2007. "Locating a Space for Ethics to Appear in Decision-Making: Privacy as an Exemplar." *Journal of Business Ethics* 70(3): 221–234.

Borna, Shaheen, and Stephen Avila. 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.

Bowie, Norman E., and K. Jamal. 2006. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?" *Business Ethics Quarterly* 16(3): 323–342.

Brenkert, George. 1981. "Privacy, Polygraphs, and Work." *Business and Professional Ethics Journal* 1: 23.

Brin, David. 1998. *The Transparent Society*. Reading, MA: Perseus Books.

Chen, Chau-Kuang, and John Hughes. 2004. "Using Ordinal Regression Model to Analyze Student Satisfaction Questionnaires." *IR Applications*, Volume 1. http://www.airweb.org/page.asp?page=554

Culnan, Mary J., and Pamela K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10(1): 104–115.

Culnan, Mary J. and Robert J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59(2): 323–342.

Dane, Eric, and Michael G Pratt. 2007. "Exploring Intuition and Its Role in Managerial Decision Making." *Academy of Management Review* 32(1): 33–54.

DeGeorge, Richard T. 2003. *The Ethics of Information Technology and Ethics*. Cambridge, MA: Blackwell Publishers.

Elgesem, David. 1999. "The Structure of Rights in Directive 95/46/EC." *Ethics and Information Technology* 1: 283–293.

Federal Trade Commission (FTC). 2010. A Preliminary FTC staff report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (December 1, 2010). http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Floridi, Luciano. 2005. "The Ontological Interpretation of Informational Privacy." *Ethics and Information Technology* 7(4): 185–200.

———. 2006a. "Information Ethics, Its Nature and Scope." *Computers and Society* 36(3): 21–36.

———. 2006b. "Four Challenges for a Theory of Informational Privacy." *Ethics and Information Technology* 8(3): 109–119. .

Fried, Charles. 1984. "Privacy." In *Philosophical Dimensions of Privacy: An Anthology*. Edited by Ferdinand D. Schoeman. Cambridge: Cambridge University Press.

Ganong, Lawrence H., and Marilyn Coleman. 2006. "Multiple Segment Factorial Vignette Designs." *Journal of Marriage and Family* 69(2): 455–468.

Goffman, Erving. 1978. *The Presentation of Self in Everyday Life.* Garden City, NJ: Anchor Doubleday.

Hoofnagle, Chris Jay, Jennifer King, Su Li, and Joseph Turow. "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

Jasso, Guillermina. 2003. "Factorial Survey Method (Rossi's Method)." In *The Sage Encyclopedia of Social Science Research Methods*, Volume 1. Edited by Michael Lewis-Beck, Alan Bryman, and Tim Futing Liao. Thousand Oaks, CA: Sage Publications.

———. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments." *Sociological Methods and Research* 343: 334–423.

Jiang, Xiaoqian. 2002. "Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the

Social." Presented at the 4th International Conference on Ubiquitous Computing (UBICOMP 2002), Gotenborg, Sweden.

Jonassohn, Kurt, Allan Turowetz, and Richard Gruneau. 1981. "Research Methods in the Sociology of Sport: Strategies and Problems." *Qualitative Sociology* 4(3): 179–197.

Katz, Nancy, and George Koenig. 2001. "Sports Teams As a Model for Workplace Teams: Lessons and Liabilities." *Academy of Management Executive* 15(3): 56–69.

Keidel, Robert W. 1987. "Team Sport Models as a Generic Organizational Framework." *Human Relations* 40: 591–612.

Kennedy, Peter. 2003. *A Guide to Econometrics*, 5th Edition. Cambridge, MA: MIT Press.

Koehn, Daryl. 2003. "The Nature of and Conditions for Online Trust." *Journal of Business Ethics* 43(1/2): 3–19.

Lehavot, Karen. 2009. "'MySpace' or Yours? The Ethical Dilemma of Graduate Students' Personal Lives on the Internet." *Ethics and Behavior* 19(2): 129–141.

Lessig, Lawrence. 1998. *The Architecture of Privacy*. The Berkman Center for Internet and Society at Harvard University web site: http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf.

———. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Loch, Karen D., Sue Conger, and Effy Oz. 1998. "Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics." *Journal of Business Ethics* 17(6): 653–663.

Lynch, John. 1983. "The Concept of External Validity." *Journal of Consumer Research* 9(3): 240–244.

March, James G., and Herbert A. Simon. 1958. *Organizations*. New York: Wiley.

Martin, Kirsten. 2010. "Privacy Revisited: From Lady Godiva's Peeping Tom to Facebook's Beacon Program." In *Ethical Issues in E-Business: Models and Frameworks*. Edited by D. E. Palmer. Hershey, PA: IGI Global.

Marwick, Alice E., Diego Murgia-Diaz, and John G. Palfrey. "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, James. 1997. "Towards a Theory of Privacy in the Information Age." *Computers and Society* (Sept): 27–32.

Moore, Adam D. 2000. "Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy." *Business Ethics Quarterly* 10(3): 697–709.

———. 2003. "Privacy: Its Meaning and Value." *American Philosophical Quarterly* 40(3): 215–227.

Nissenbaum, Helen. 1997. "Toward an Approach to Privacy in Public: Challenges of Information Technology." *Ethics and Behavior* 7(3): 207–219.

———. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79(1): 119–158

———. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

Nock, Stephan, and Thomas M. Gutterbock. 2010. "Survey Experiments." In *Handbook of Survey Research*, Second Edition. Edited by James Wright and Peter Marsden. Bingley, UK: Emerald.

Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technologies.* Princeton, NJ: Princeton University Press.

Persson, Anders H., and Sven Ove Hansson. 2003. "Privacy at Work—Ethical Criteria." *Journal of Business Ethics* 42(1): 59–70.

Peslak, Alan R. 2005. "An Ethical Exploration of Privacy and Radio Frequency Identification." *Journal of Business Ethics* 59(4): 327–345.

Pollach, Irene. 2005. "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent." *Journal of Business Ethics* 62(3): 221–235.

Rachels, James. 1975. "Why is Privacy Important?" *Philosophy and Public Affairs* 4(4): 323–333.

Reiman, Jeffrey H. 1975. "Privacy, Intimacy, and Personhood." *Philosophy and Public Affairs* 6(1): 26–44.

———. 1995. "Driving to the Panopticon." *Santa Clara Computer and High Technology Law Journal* 11(1): 27–44.

Roman, Sergio, and Pedro J. Cuestas. 2008. "The Perceptions Of Consumers Regarding Online Retailers' Ethics And Their Relationship With Consumers' General Internet Expertise And Word Of Mouth: A Preliminary Analysis." *Journal of Business Ethics* 83(4): 641–656.

Rosen, Jeffrey. 2001. *The Unwanted Gaze: The Destruction Of Privacy In America.* New York: Vintage Books.

Rossi, Peter, and Stephen Nock, eds. 1982. *Measuring Social Judgments: The Factorial Survey Approach.* Beverly Hills: Sage.

Sama, Linda M., and Victoria Shoef. 2002. "Ethics on The Web: Applying Moral Decision-Making To The New Media." *Journal of Business Ethics* 36(1/2): 93–103.

Schoeman, Ferdinand. 1984. Privacy: Philosophical Dimensions of the Literature. In *Philosophical Dimensions Of Privacy: An Anthology.* Edited by F. D. Schoeman. Cambridge: Cambridge University Press.

Schonsheck, Jonathan. 1997. "Privacy and Discrete 'Social Spheres.'" *Ethics and Behavior* 7(3): 221–228.

Schwartz, Barry. 1968. "The Social Psychology of Privacy." *The American Journal of Sociology* 73(6): 741–752.

Shaw, Thomas R. 2003. "The Moral Intensity of Privacy: An Empirical Study Of Webmasters' Attitudes." *Journal of Business Ethics* 46(4): 301–318.

Simon, Herbert. 1945. *Administrative Behavior: A Study of Decision-Making Processes In Administrative Organization.* New York: Free Press.

Singleton, Solveig. 1998. "Privacy as Censorship." *Cato Institute: Policy Analysis* 295.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20(2): 167–196.

Solove, Daniel J. 2006. "A Taxonomy Of Privacy." *University of Pennsylvania Law Review* 154(3): 477.

———. 2007. "'I've Got Nothing To Hide,' And Other Misunderstandings Of Privacy." *San Diego Law Review* 44.

Stone, Dianna L., and Debra Kotch. 1989. "Individuals' Attitudes Toward Organizational Drug Testing Policies And Practices." *Journal of Applied Psychology* 74: 518–521.

Stone, Eugene F., and Dianna L. Stone. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, And Protection Strategies." *Research in Personnel and Human Resources Management* 8: 349–411.

Tavani, Herman T. 2008. "Floridi's Ontological Theory Of Informational Privacy: Some Implications And Challenges." *Ethics and Information Technology* 10(2/3): 155–166.

Taylor, Brian J. 2006. "Factorial Surveys: Using Vignettes to Study Professional Judgment." *British Journal of Social Work* 36: 1187–1207.

Tversky, Amos, and Daniel Kahneman. 1974. "Judgment under Uncertainty: Heuristics And Biases." *Science* 185: 1124–1131.

Wallander, Lisa. 2009. "25 years of Factorial Surveys in Sociology: A Review." *Social Science Research* 38: 505–520.

Warren Samuel D., and Louis D. Brandeis. 1890. "The Right To Privacy." *Harvard Law Review* 4(5): 193–220.

Weick, Karl. 1995. *Sensemaking n Organizations.* Thousand Oaks, CA: Sage Publications.