2014

Areas of Privacy in Facebook: Expectations and Value

Katherina Glac Ph.D.
University of St. Thomas, Minnesota, glac6548@stthomas.edu

Dawn Elm
University of St. Thomas, Minnesota

Kirsten Martin
George Washington University

Areas of Privacy in Facebook

Article *in* Business & professional ethics journal · January 2014

DOI: 10.5840/bpej2014111113

CITATIONS
3

READS
64

3 authors, including:

Kirsten E. Martin
George Washington University
34 PUBLICATIONS **249** CITATIONS

SEE PROFILE

Business & Professional Ethics Journal
doi:
Online First:

Areas of Privacy in Facebook: Expectations and Value

Katherina Glac
University of St. Thomas, Opus College of Business

Dawn R. Elm
University of St. Thomas, Opus College of Business

Kirsten Martin
George Washington University School of Business

Abstract: Privacy issues surrounding the use of social media sites have been apparent over the past ten years. Use of such sites, particularly Facebook, has been increasing and recently business organizations have begun using Facebook as a means of connecting with potential customers or clients. This paper presents an empirical study of perceived privacy violations to examine factors that influence the expectations of privacy on Facebook. Results of the study suggest that the more important Facebook is to users, the more likely they are to perceive privacy violations and the more likely those violations are to be considered serious. Furthermore, how information is used is more important than the way this information is accessed.

Key Words: privacy, social media, Facebook

Introduction

The use of social media, and Facebook in particular, is popular with U.S.-based corporations (Facebook). Businesses large and small have come to rely on social media for public relations, marketing, and recruiting. For example, 83 percent of marketers say social media is important (Stelzner 2012) and 57 percent of small businesses find social media somewhat or highly valuable (Maltby and Ovide 2012). For small businesses, Facebook and Twitter are the most popular social

Correspondence may be sent to Katherina Glac, kglac@stthomas.edu.

network sites with 90 percent and 70 percent penetration respectively (Reilly 2012). And in Europe, 69 percent of executives find it is important to integrate social media into marketing and business plans (CNBC 2012).

While popular, social media also presents hurdles for business. Of small businesses using Facebook, 58 percent have trouble managing Facebook (Herzog 2012). This is not surprising as social media challenges privacy expectations in the peer-to-peer communication of users and the different relationships forming the bases of the technology (Tufekci 2008). The management of online privacy and the development of social media policies by corporations are raising increasing ethical and social responsibility concerns for businesses as well; (Kaupins, Coco, and Little 2012; Pollach 2011). Actively managing the privacy expectations of these stakeholders in the business environment is important from a legal perspective as well. For example, courts both in the US as well as internationally have repeatedly looked at how corporate privacy policies might or might not create expectations of privacy by employees and customers (Abril, Levin, and Del Riego 2012; Sprague 2012).

Facebook has become a significant factor in the current social communication structure of today's culture. It is more uncommon to find individuals and companies that do not have a Facebook account than vice versa. Facebook has been involved in debates surrounding privacy at various times since its inception (Electronic Privacy Information Center 2013). However, serious privacy concerns do not seem to be a significant deterrent for existing and new Facebook users as the number of Facebook users has continued to soar over the past years. Previous research (Martin 2012) has confirmed that Facebook users generally have lower expectations for privacy on Facebook as compared to other areas of their lives. However, while on average those privacy expectations were lower, that research found significant variations of privacy expectations among subgroups of users as well as among types of content.

Simultaneously with the apparent reduction of privacy expectations among the general public comes an increasing perception among corporations that Facebook users have low expectations of privacy in this setting and that "anything goes" (Abril 2010) with regard to using information from Facebook. Increasingly social media usage, and in particular Facebook, is being done in the corporate setting for purposes of hiring and firing (Brandenburg 2008; Elzweig and Peeples 2009) or marketing (LaPointe 2012). However, other research has shown that while social media users might have lower expectations of privacy, they still value privacy and are concerned or even feel helpless in the face of

increased privacy erosion (Christofides, Muise, and Desmarais 2009; Levin and Abril, 2009; Tan, Qin, Kim, and Hsu 2012).

This contradictory observation that individuals share more and more information about themselves but at the same time seem to be overall concerned about their privacy online increases the relevance of previous findings about differences in perceived value and expectations of privacy within the larger Facebook domain. If in fact not everything "goes" in all areas of Facebook, then more research is needed to obtain a more accurate picture of what does "go" within Facebook and under what circumstances. Any findings about differences in perceived value and expectations of privacy within the larger Facebook domain could result in important guidelines for corporations on how to design policies regarding use of information contained on Facebook.

The penetration of Facebook as a marketing, public relations, recruiting, and strategic tool for business forms the impetus for the paper and leads to our goal in our paper: This paper tries to fill part of the information gap outlined above and focuses on exploring privacy expectations and valuation in the context of the social network site Facebook. The theoretically generalizable findings identify drivers of privacy attitudes on Facebook so that businesses utilizing Facebook can better meet the privacy expectations of users. Our research goes beyond existing work in two ways. First, we extend the one-dimensional privacy definitions used frequently in other research on privacy, in which respondents were left to interpret what privacy means, simply looked at propensity to use privacy settings, or examined the perceived risks associated with breaches of privacy (Christofides et al., 2009; Hoadley, Xu, Lee, and Rosson 2010; Miyazaki and Fernandez 2001).

Second, we move beyond the notion of whether there is or is not an expectation of privacy to how much that privacy is valued, i.e., how serious a breach of the privacy expectation is. Adding the value dimension connects our work to that done by Solove (2007) in the area of law who develops this idea of value of privacy. The goal behind adding the privacy value dimension to this research is the exploration of whether the lower expectations of privacy in some areas are compensated by higher expectations and higher value of privacy in some other areas of Facebook, or whether there is a general decline in the value of privacy overall.

Privacy Research

Conceptions of Privacy

Various scholarly disciplines ranging from philosophy, psychology, law to sociology have contributed to the discussion around privacy thus adding significant complexity. As Solove (2002, 1082) points out "the widespread discontent over conceptualizing privacy persists even though the concern over privacy has escalated into an essential issue for freedom and democracy." In summarizing the conceptions of privacy found in the various literatures, Solove points to six different conceptions that each capture a different aspect of privacy.

On one hand there are conceptions including the right to be let alone (Warren and Brandeis 1890) and shielding information about and access to ourselves and our intimate relationships (e.g., Bok 1983; Breckenridge 1970; Etzioni 1999; Gerstein 1984; Godkin 1890; Posner 1981; Rosen 2000) that could be grouped under the notion of what Whitman (2004) has called "liberty." The notion of liberty, according to Whitman, is the predominant view of privacy in America and has its origins in "the right to freedom from intrusion by the state, especially in one's own home" (2004, 1161). This conceptualization has often been operationalized as the right to control information by an individual as a means of ensuring his or her freedom.

On the other hand there are conceptions connected to respect, dignity, and personhood: "the ability to exercise control over information about oneself [and] the protection of one's personality, individuality, and dignity" (Solove 2002, 1092).[1] Bloustein (1964, 1006) even goes as far as saying that a violation of privacy results in "stripping the individual naked of his human dignity by exposing his personal life to public scrutiny." In the psychology literature this notion has been reflected in the influential work of Altman (1975), Westin (1967), and Margulis (1977; 2003). Altman and Westin suggest that privacy functions as a means of self-evaluation as well as contributing to the development of self-identity and individuality. Westin (1967), in particular, argues that privacy provides opportunities for self-assessment and experimentation and is important to individuals because it provides experiences that support and further normal psychological functioning, development and relationships. Later work examined the linkage between privacy concerns (or violation perceptions) and identity in the age of online communication (Ellison, Heino, and Gibbs 2006; Kobsa, Patil, and Meyer 2012; Shroff and Fordham 2010). Recent work by Stein, Galliers, and Markus (2013) specifically examined the creation of identity through technology in the workplace and found that different information technology uses are related to different types of preferred "selves" individuals adopt at work. This could have

implications for Facebook usage as a type of technology that contributes to the development of preferred identities of users.

These two overarching notions of privacy, namely liberty and dignity, capture two different ends of a spectrum: "Privacy as dignity protects the 'me'; privacy as freedom protects the 'I.' Privacy as dignity safeguards the socialized aspects of the self; privacy as freedom safeguards the spontaneous, independent, and uniquely individual aspects of the self" (Post 2001, 2095). While the dignity conception of privacy that is focused on shaping, maintaining and protecting a certain public image is more predominant in Europe (Whitman 2004), it takes on particular relevance in the context of social media: there is less of a distinct physical "home" to shield individuals on the internet (and thus capture the liberty aspect of privacy), but there is also an increased emphasis on presentation and maintenance of relationships and personas through personal "profiles" and "pages." This represents an extension of traditional impression management using computer-mediated communication (Bozeman and Kaemar 1997; Goffman 1959; Kobsa et al. 2012). In contexts where face-to-face relationships are not always present, privacy becomes furthermore instrumental in establishing fairness and trust in interpersonal relationships (Koehn 2003).

Thus, in this paper we build on the two overarching privacy concepts of liberty/freedom and dignity. The former, as indicated above, relates mainly to issues of control and access to information. The latter relates to image or persona creation and maintenance. While research around privacy has mostly looked at the occurrence of a privacy violation in specific circumstances, i.e., the question "has privacy been violated by an act"? has been at the forefront, not all violations are created equal. An important additional element in discussions around privacy is the notion of "value" or "seriousness." Bloustein's (1964) discussion of the seminal work by Warren and Brandeis (1890) points to this important distinction. He argues that traditional privacy "torts" in law serve to protect important underlying interests, which he identifies as "preserving human dignity and individuality" (Bloustein 1964, 1005)—and based on our discussion above we might add control and access to information. Using an example of the publication of a woman's picture without her consent that makes her beauty famous overnight much to her delight he argues: "Has privacy been violated when there is no personal sense of indignity and the commercial values of name or likeness have been enhanced rather than diminished? I believe that in such a case there is an invasion of privacy, although it is obviously not one which will be sued on" (Bloustein, 1964, 990). What Bloustein points to here is that an act can violate privacy because it affects the underlying interests, but it might not be considered

harmful or serious to warrant litigation. Thus there is a distinction between violation of privacy and the value privacy has in preventing harm. Since this distinction between violation and value has been either overlooked or conflated in previous work, we assess each component separately in the present study.

Privacy Research on Expectations and Influences

Empirical research reflects and confirms the importance of the two main privacy categories of liberty and dignity to various degrees. For example, Abril (2010) has proposed four variables influencing expectations of privacy: content or what is disclosed, context such as social relationships or closeness of a group, control over dissemination of information, and the existence of a contract or cues that transmit expectations about behavior. Margulis (1979) and Johnson (1974) have suggested that the content of the information is particularly relevant as a factor in influencing privacy expectations. Additional work on the perception of invasion of privacy in hiring decisions suggests that control over disclosure in the hiring process and the outcome of disclosure (Fusilier and Hoyer 1980) are significant predictors of perceptions of privacy violations as well. Recent research in information technology regarding awareness systems (such as instant messaging, use of social media sites and other online communication methods) confirms this perspective, determining that relationship with the information recipient, use and purpose of the information, context, and sensitivity of the information are all factors that affect the perception of privacy violations (see Kobsa et al. 2012).

While the above research indicates that, in general, control of and access to information as well as maintenance of image or personas are significant factors in privacy evaluations, more recent research on both identity management and privacy expectations indicates more nuance and has suggested that privacy and identity are contextually dependent (Martin 2012; Nissenbaum 2004; Shroff and Fordham 2010). Such perspectives suggest that privacy norms or expectations of an individual or group are dependent on the context of the "space" in which the privacy is being evaluated.

Martin built her work specifically on social contract theory, which is compatible with the liberty/dignity conception of privacy. Social contract theory suggests that various communities set their own behavioral norms within certain boundaries and under certain procedural conditions. In that sense communities, such as social media communities like Facebook, might create norms that interpret the extent of liberty around personal information or image maintenance for specific situations. In focusing on one such specific situation or "space," namely

social media, we explore in our paper to what extent the privacy conceptions of liberty and dignity play a role in driving privacy expectations in that space.

Hypotheses

We build our hypotheses about the factors that influence privacy expectations as well as perceived privacy value in the specific social media domain of Facebook on the overarching privacy conceptions of liberty and dignity. On a general level, based on the conceptualization that privacy means having control over and determining access to personal information for the purpose of maintaining different relationships and identities, we expect that individuals using Facebook will perceive privacy violations, as well as their severity, based on the extent they control dissemination of information and the extent to which Facebook is important in creating relationships as well as shaping and maintaining a certain kind of identity or image about themselves. The factorial survey design used for our study offers a unique opportunity to examine how the different factors work together in shaping privacy expectations and valuation.

Identity Maintenance

Various studies have documented the important role social media and particularly Facebook plays in identity maintenance. Christofides, Muise, and Desmaris (2009) found that the need for popularity was a significant predictor of disclosure on Facebook. Levin and Abril (2009) surveyed 2500 young adults about their online information sharing they found that the subjects were "primarily concerned about privacy as it relates to the presentation of the self" (2009, 1045). Hoadley, Heng, Lee, and Rosson (2010) found that the use of Facebook was primarily for self-presentation and relationship maintenance and that this function was an important reason for the upset many users perceived at the introduction of the NewsFeed feature, which influenced the users' "abilities to express their identities for others to see and interpret" (Hoadley et al. 2010, 53). Turkle's (2011) work examines the use of online worlds as "identity workshops" (12) where an individual's online life re-shapes the self. Her interviews with high school and college Facebook users indicates that presentation anxiety exists regarding who you will *be* on Facebook as a driving force for sharing information on the site.

Given that in the Facebook context the maintenance of specific social identities and relationships is the main goal of information sharing, a violation of privacy might be more likely and more severe the more pronounced the interest is that it is protecting. In other words, if individuals use Facebook

extensively and with a significant share of their social circle, the privacy interest of identity and relationship maintenance is more pronounced and violations of privacy might result in more opportunity for harm and thus be evaluated more seriously—i.e., privacy in such context has a higher "value." On the other hand, if an individual has only very limited exposure to Facebook and maintains relationships and identities primarily outside of social media, privacy violations in situations where information is accessed by someone for whom it might not have been intended and the resulting harm to the individual should also be limited. Thus, hypothesis 1 and 2 propose:

> **H1**: The more exposure an individual has to Facebook the more likely it is that a privacy violation will be perceived if information is accessed by someone else.
>
> **H2**: The more exposure an individual has to Facebook the more likely it is that a privacy violation will be perceived as serious if information is accessed by someone else.

Even though some individuals use Facebook extensively, not all information that is disclosed by an individual is the same. Some information might relate to locations they visited or pictures of their friends that they liked, neither of which is particularly closely related to the individual's image (though certainly taken in their entirety the likes and links shared all create an individual's identity). However, some types of information can be more immediately relevant in self-presentation, such as relationship status, sexual orientation, purchasing behavior, social activities (e.g., partying), etc. Thus, in line with the earlier argument about the likelihood and severity of privacy violations being determined by the significance of the underlying interest (here image creation and maintenance), we would thus expect that the more some shared information is connected to an individual's identity, the more likely a violation is to occur and to be considered serious. Thus hypotheses 3 and 4 propose:

> **H3**: The more information of a Facebook user is connected to his/her identity, the more likely it is that a privacy violation will be perceived if information is accessed by someone else.
>
> **H4**: The more information of a Facebook user is connected to his/her identity, the more likely it is that a privacy violation will be perceived as serious if information is accessed by someone else.

In addition, assuming that individuals present different identities in different relationship contexts, we would also expect privacy expectations to be higher

and privacy more valued in situations in which the party accessing information is supposed to be presented with a different facet (or version) of an individual's identity than the accessed information actually supports (Westin 1967; Margulis 2003; Shroff and Fordham 2010; Kobsa et al. 2012). For example, Shroff and Fordham (2010) suggest that identity is contextually based on the number of roles humans play in various interactions: "Context affects both the range of information you might reasonably be asked to provide and the selection you make about what you willingly reveal" (301). In other words, we would expect that an individual would not find it problematic if a close friend saw pictures of a recent party the individual attended, but that an employer seeing such pictures would be perceived as a serious violation of privacy because the identity presented to an employer presumably focuses on professional personality attributes. Thus we expect privacy expectations to vary depending on the type of relationship between the Facebook user and the person accessing the information.

> **H5**: The closer the relationship between the Facebook user and the person accessing that information, the less likely it is that a privacy violation will be perceived when the information is accessed by someone else.
>
> **H6**: The closer the relationship between the Facebook user and the person accessing that information, the less serious a privacy violation will be perceived when the information is accessed by someone else.

Control Over and Determining Access To Personal Information

Nowak and Phelps (1995) focus on the interactional aspect of online activity and argue that individuals exchange their personal information for economic or social benefits. Youn (2005) confirmed that if more benefits from information disclosure were provided, the users were then willing to provide more information. To allow targeted exchange, individuals have to be able to maintain control over and be able to limit access to personal information and to determine how such information is used in the end. In line with the liberty conception of privacy discussed earlier, Miyazaki and Fernandez (2001) confirmed that a lack of control was a significant factor in perception of privacy violation in their study of consumer online shopping. Subjects suggested that unsolicited email and potential tracking behavior of web-based marketers was troublesome. Similarly, in a study of 742 internet-using households Malhotra, Kim, and Agarwal (2004) found that the dimensions influencing internet users' information privacy concerns are the way personal information is collected, control over the collected information, and awareness of how the collected information is used.

Following previous research on the importance of control over information as well as its use (Martin 2012; Youn 2005; Fusilier and Hoyer 1980), we assume that the way in which information is obtained by someone will affect if and how seriously an individual will perceive a privacy violation. A Facebook user can, to some extent, control who has direct access to information by controlling the connections and privileges Facebook friends have to one's profile. Thus, in theory, the Facebook user would know which friends see which types of information. However, if someone else uses the account of an individual's Facebook friend, or if user data is sold to third parties, then the individual can no longer control who receives that information. Also, if the information is used for a purpose outside of the social relationship in which the information was created or for which it was intended, the underlying privacy interest of control is equally affected. This premise is consistent with the work of Malhotra et al. (2004) who found that how collected online information is used influences privacy concerns. The potential for harm from the loss of control is also dependent on type and purpose of access (Youn 2005). Taken together, hypotheses 7 through 10 thus propose:

H7: The type of access to the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was accessed through one's own account the perception of a privacy violation will be less likely than if the information was accessed by using someone else's account or purchasing that access.

H8: The type of access to the information of a Facebook user will affect the seriousness of a perceived privacy violation such that if the information was accessed through one's own account a privacy violation will be perceived as less serious than if the information was accessed by using someone else's account or purchasing that access.

H9: The type of use of the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was used for personal reasons the perception of a privacy violation will be less likely than if the information was accessed for professional or business reasons.

H10: The type of use of the information of a Facebook user will affect the seriousness of a perceived privacy violation such that if the information was used for personal reasons a privacy violation will be perceived as less serious than if the information was accessed for professional or business reasons.

Methodology

Factorial Survey Design

This research aims to deconstruct what factors influence privacy perceptions and valuation in the Facebook domain. Toward this end, 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 are 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). 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 as to judgments of privacy.

The vignettes were constructed by varying several factors along dimensions or levels. A deck of vignettes for each respondent was randomly created from the entire set of vignettes. For each rated vignette, the associated rating, factor levels, and the vignette script was preserved, as well as the vignette sequence number. The vignette format is also provided in the tables below along with a sample vignette and the vignette template.

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 have relatively simple mappings onto the constructs of concern" (Lynch 1982, 233). Here, we representatively sampled factors in order to test the hypotheses based on the privacy scholarship explored above.

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 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) measures of an individual's exposure to Facebook, and (2) privacy factors that may vary in importance across situations in which Facebook is used. The number of vignettes that can be created out of the possible factor combinations is determined by the number of factors and the levels of these factors (in our case 4 factors and 3–5 levels each = $5 \times 3 \times 3 \times 3$ or 135). While this represents a large number of possible combinations, every respondent only receives a maximum of 30 vignettes. However, each vignette represents an observation (or n) and therefore the resulting dataset is the product of respondents and vignettes per respondent.

The following is the basic structure of a vignette with placeholders indicating a factor. The factors were systematically varied to create all possible combinations of factors, resulting in 135 unique vignettes. A sample vignette is included below.

> **General Vignette Format**
>
> While updating [type of access], Anna saw a wall post from [closeness of relationship], talking about [type of information]. The next day, Anna shared the information about Patricia with [type of use].
>
> **Vignette Example**
>
> While updating **her own Facebook account**, Anna saw a wall post from **Patricia, a close friend**, talking about **getting drunk at a recent party**. The next day, Anna shared the information about Patricia with **Mary, the Human Resource Manager at the local bike shop where Anna works, because Patricia was being interviewed for a job there**.

Rating Task (Dependent Variables)

Each participant was presented with 30 vignettes randomly drawn from the vignette universe. Vignettes were presented on a computer in a behavioral research laboratory. Each participant had the opportunity to exit the study after a set of 10 vignettes, which is aimed at reducing respondent fatigue (Nock and Gutterbock 2010). For each vignette, respondents were given two rating tasks. They were presented with the vignette and then asked "Was it OK for Anna to use/share the information the way she did?" using a response scale of 1 to 7, with 1 being "absolutely not ok" and 7 being "absolutely ok." The response to this question assessed whether the respondent perceived the occurrence of a privacy violation or not (dependent variable 1). Respondents were also asked

"How SERIOUS was it that Anna used/shared the information the way she did?", again with a response scale of 1 to 7, this time 1 being "very serious" and 7 being "not serious at all." The second question assessed how serious a privacy violation was (dependent variable 2).

Table 1 lists the vignette factors and Table 2 lists the other variables assessed in our study, which are demographics, measures for importance of Facebook, privacy violation occurrence, and violation serious ness.

TABLE 1: Vignette Factors

	Factors	Dimensions		Operationalized as
1	Closeness of relationship with information recipient	0	close Facebook friend	Patricia, a close friend
		1	classmate	Liz, one of her classmates from chemistry 101
		2	coworker	Barbara, a coworker from her part-time job at the local bike shop
		3	employer	Lauren, one of the employees at the local bike shop Anna owns
		4	company	Jamie, a customer at the local bike shop Anna owns
2	Type of access to information	1	through own Facebook account	her own Facebook account
		2	using someone else's account	her sister's Facebook account
		3	purchased from Facebook*	While looking at the data provided by Facebook
3	Type of information accessed	1	social behavior	getting drunk at a recent party
		2	purchasing behavior	purchasing an expensive necklace
		3	personal characteristics—here sexual orientation	a romantic trip with her same sex partner
4	Use of information	1	personal use	when Anna was talking to her mother, she told her about what she read on Patricia's wall post
		2	business use	Anna entered this information about Liz under "sexual orientation" into the direct mailing database of the bike shop where Anna works.
		3	professional use	Anna shared this information with Mary, the Human Resource Manager, at the local bike shop where Anna works because Patricia was being interviewed for a job there

*in scenarios in which access is purchased the scenarios were worded slightly differently to maintain a consistent logic in the vignette.

TABLE 2: Variables Assessed

Variable	Measure
Privacy violation (Dependent Variable 1)	"Was it OK for Anna to use/share the information the way she did?" with a response scale of 1 to 7 with 1 being "absolutely not ok" and 7 being "absolutely ok."
Seriousness of privacy violation (Dependent Variable 2)	"How SERIOUS was it that Anna used/shared the information the way she did?", with a response scale of 1 to 7, this time 1 being "very serious" and 7 being "not serious at all."
Importance of Facebook in an individual's life	Number of hours spent on Facebook Number of Facebook friends
Age	Numerical entry
Gender	Male/Female
Ethnicity	• Caucasian • African-American • Asian • Hispanic • Other
Work experience	• Some work experience • Internship • Part-time work • Full-time work
International student	Yes/No
Year of study	• Freshman • Sophomore • Junior • Senior

Sample

The participants for this study were 92 undergraduate students recruited from the student body of a large private Midwestern university via posters in dorms, ads in an online bulletin, and direct contacts to students who had previously participated in research studies. Undergraduate students are ideal subjects for studying privacy perceptions on Facebook because they are the original, as well as one of the most active, user groups on Facebook. The students received $7 as compensation for their participation. Out of 92 respondents who answered any vignettes, 78 answered all 30 vignettes, 3 respondents answered 20, and 11 respondents answered 10 vignettes or fewer. Taken together, the 92 respondents answered a total of 2710 vignettes, which constitutes the total number of observations for our analyses (i.e., n).

Of the 92 undergraduate students participating in our study, 43.8% were male, the mean age was 20.7 years, 9% were freshmen, 20% sophomores, 52% juniors, and 19% seniors. On average, the participants spent 7.6 hours a week on Facebook (max. 35 and min. 0) and had 558 Facebook friends (max. 2500 and

min. 0). 74% of participants indicated their ethnicity as Caucasian, 4% African-American, 12% Asian, 1% Hispanic, and 13% selected "other." Overall 6% of participants were international students. Most students (96%) indicated they had some sort of work experience: 37% had completed internships, 63% had worked part-time, and 35% had full-time work experience.

Results

In testing the hypotheses, Ordinary Least Squares (OLS) regression was used to identify the factors that influence the assessment of privacy violation and seriousness of that valuation (the dependent variables).

Hypotheses 1 and 2 predict that *the more exposure an individual has to Facebook the more likely it is that a privacy violation will be perceived and the violation will be considered more serious*. To test hypotheses 1 and 2, the respondents' exposure to Facebook needed to be operationalized. To operationalize exposure, the respondents were ranked into quintiles (20%-tiles) for the number of friends they had on Facebook and the number of hours they spent on Facebook per week. This resulted in the five tiers of Facebook Friends and Hours as illustrated in Table 3.

TABLE 3: Tiers of Respondents' Facebook Friends and Hours.

Quintile	FBFriends5		FBHours5	
	Mean Friends	Mean Hours	Mean Friends	Mean Hours
1	138.2	6.9	514.5	1.4
2	368.5	6.4	534.7	3.1
3	507.7	5.4	466.2	6.1
4	618.9	7.8	671.4	9.3
5	1269.0	10.4	715.5	17.7

Respondents who had high exposure to Facebook as compared to the rest of the sample (designated as High FB exposure) were those in the top 2 quintiles or top 40% of both friends and hours (with variables FBFriends5 and FBHours5 = 4 or 5). Respondents who did not have a high exposure to Facebook (designated as Very Low FB exposure) were those in the bottom 20% of Facebook friends and hours (FBFriends5 and FBHours5 = 1). Those with high exposure and very high exposure to Facebook (the top 40th percentile and top 20th percentile respectively) are more likely to be female and younger (see Table 4). Respondents with Very High FB exposure are 19.50% male compared the 47.58% male for all respondents. Very High FB exposure respondents are

2.65 years in school (between sophomores and juniors) as compared to 3.26 years for Very Low exposure respondents. These descriptive statistics might be an indication that socialization, which increasingly operates through the use of social media, plays an important part of college life in the early years. In later college years the focus seems to shift away from social media.

TABLE 4: Demographics of Sample by Facebook Identity Measure

	High v. Low Identity	DV = Violation	CV = Serious	Age	Student	Male
Bottom 20% hrs&Frnds	Very Low Identity	3.72	3.71	21.13	3.26	97.00%
Bottom 40% hrs&Frnds	Low Identity	3.50	3.48	20.65	2.94	69.18%
Top 40% hrs&Frnds	High Identity	3.09	3.24	20.99	2.93	46.03%
Top 20% hrs&Frnds	Very High Identity	3.11	3.05	20.19	2.65	19.50%
	All Respondents	3.37	3.44	20.69	2.83	43.82%
	New Respondents	3.46	3.42	21.10	2.85	47.58%
	Original Respondents	3.29	3.46	20.28	2.81	40.16%

Respondents with greater Facebook exposure (greater hours and friends) had *lower* privacy violation ratings and lower seriousness of the violation ratings (see Table 4). Given the response scales in which 1 indicated that a violation did occur (or was serious) while 7 indicated that a violation did not occur (or was not serious), the results mean that *violations were more likely and more serious the more an individual was exposed to Facebook*. Very High FB exposure respondents had an average Violation rating of 3.11 and Seriousness rating of 3.05 (compared to 3.72 and 3.71 for Very Low FB exposure respondents).

In addition, the number of hours and friends were analyzed individually. The greater the number of Facebook friends, the lower the Violation rating of the vignettes as seen in Table 5 (FBFriends5 = −0.124 (p = 0.00) for the Violation DV and −0.081 (0.00) for the Seriousness DV). A *greater number of FB Friends has a* ***negative*** *impact on both rating tasks such that respondents judged vignettes to be more of a violation and more serious when they had more friends*. However, the more hours a respondent spent on Facebook, the less vignettes were considered a violation and violations were judged less serious. Facebook hours has no impact on both rating tasks as seen in Table 5.

The findings thus *do* support the prediction in Hypotheses 1 and 2 that the more an individual is exposed to Facebook (as measured by the number of friends and hours spent on Facebook) the more likely it is that a privacy violation will be perceived and the more serious the violation.

Hypotheses 3 and 4 predict that *the more information of a Facebook user is connected to his/her identity, the more likely it is that a privacy violation will be perceived and that violations will be considered serious*. To test the remaining hypotheses, both rating tasks were regressed on the factors of the vignettes as depicted in Table 5. While the type of the information is important to privacy judgments as shown in Table 5, personal information (0.761, p = 0.00) has a *positive* impact on the Violation rating task relative to purchase information and social information. Similarly, personal information (1.036, p = 0.00) has a *positive* impact on the Seriousness DV relative to purchase information; in other words, respondents found access to personal information less serious of a violation than purchase and social information. The findings thus *do not conclusively* support the prediction in Hypotheses 3 and 4 that the more information of a Facebook user is connected to his/her identity, the more likely it is that a privacy violation will be perceived and violations will be considered serious.

Hypotheses 5 and 6 predict that *the closer the relationship between the Facebook user and the person accessing that information, the less likely it is that a privacy violation will be perceived and that violations will be considered serious*. As seen in Table 5, the type of relationship—if the person accessing the information is a classmate, coworker, employee, customer, or a friend—is *not* important to privacy judgments. The factors are *not* significant in Table 5, and all relationship types are treated the same by respondents in comparison to the Friend relationship. The findings *do not* support the prediction in Hypotheses 5 and 6 that the closer the relationship between the Facebook user and the person accessing that information, the less likely a privacy violation will be perceived and that violations will be considered serious.

Hypotheses 7 and 8 predict that *the type of access to the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was accessed through one's own account, the less likely it is that a privacy violation will be perceived and that violations will be considered serious*. The type of access can be important for privacy judgments as seen in Table 5. Access to information through the account of someone else has a *negative* impact on the Violation rating task (OtherAccess = −0.394, p = 0.00) relative to access through a personal account, which was the baseline for hypotheses 7 and 8. Respondents found that *accessing information while using*

TABLE 5: Regressions for Privacy Violation and Seriousness of Violation for all respondents.
Bold if p<.05 (not significant factors are in grey)

Likely position for Table 5 (Violation

someone else's account was a greater privacy violation than accessing information through one's own account. Purchasing access to information is also treated as more of a violation (−0.169, p = 0.04) than when using a personal account. Both OtherAccess (−0.260) and PurchaseAccess (−0.169, p = 0.02) have a *negative* impact on the Seriousness rating task as well; *respondents viewed access to information using one's own account to be less serious than accessing information through someone else's account or purchasing that information from Facebook*. The findings thus *do* support the predictions in Hypotheses 7 and 8 that the type of access to the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was

Likely position for Table 5 (Seriousness)

accessed through one's own account, it is less likely that a privacy violation will be perceived and violations will be considered less serious.

Hypotheses 9 and 10 predict that *the type of use of the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was used in a personal context it is less likely that a privacy violation will be perceived and violations will be considered less serious in comparison to using that information in a professional or business context*. Professional use was operationalized as use in a situation that had to do with hiring or promotion and business use was operationalized as use of information for direct marketing purposes. Our analyses indicate that the type of use (Business

v. Professional v. Personal) is important to privacy judgments. The factors are significant in Table 5. Personal use (1.569, p = 0.00) and Business use (0.179, p = 0.03) has a *positive* impact on the Violation rating task relative to Professional use, meaning the *vignettes with Personal and Business use were judged to be* ***less*** *of a violation than vignettes with Professional use*. In addition, both Business (0.275, p = 0.00) and Personal (1.605, p = 0.00) use have a *positive* impact on the Seriousness rating task relative to Professional use. This means that *using information in a professional context is a more serious violation of privacy than using that information in a personal or business context*.

The findings thus *do* support the prediction in Hypotheses 9 and 10 that the type of use of the information of a Facebook user will affect the likelihood of a perceived privacy violation such that if the information was used for personal reasons the less likely a privacy violation will be perceived and violations will be considered less serious in comparison to professional or business reasons.

Discussion

The testing of our hypotheses about the factors influencing the perception of privacy violations and the seriousness of those violations yielded several interesting results. First, both theoretical approaches to understanding privacy that we used to construct our hypotheses—freedom/liberty (control) and dignity—seem to be relevant in predicting privacy judgments and valuation by individuals. Hypotheses 1 through 6, which focused on the concept of privacy as dignity, found that the more an individual is exposed to Facebook, the more likely it is that access to information that is contained in Facebook will be perceived as a violation of privacy. Violations of privacy will also be considered more serious for individuals in whose life Facebook features more prominently as a means of preserving on online self. While we did not directly measure identity, we operationalized the "exposure to Facebook" variable with reference to both number of Facebook friends and hours spent on Facebook. The number of friends an individual has should be a reasonable proxy since "friending" someone on Facebook is a statement that the individual is willing to share certain information and maintain a relationship with this person. And, a separate analysis of hours and number of friends seems to indicate that the main driver behind the variable is the number of friends (however, the absence of finding an effect for number of hours does not indicate that number of hours does not play a role, as might the number of posts). The importance of the number of Facebook friends in predicting perception of privacy violation and seriousness might point toward the importance of simultaneously considering the freedom/liberty (control) aspect of privacy as

further discussed below, because presumably a larger number of friends might make it more difficult to fully control and keep track of the dispersion, access, and use of one's information by the large groups of individuals connected to a user's account.

Hypotheses 7 through 10 focused on the liberty/freedom aspect of privacy expressed as control over information dissemination. We found support for this notion of privacy as well: access to information that was obtained through an account that was not one's own or through a purchase from Facebook was more likely to be considered a serious violation of privacy, presumably because an individual cannot control the access to information if the account of an authorized "friend" is used by someone unauthorized or if the information in the account is sold by Facebook to third parties.

Furthermore, we found that privacy is also violated if information is used for a purpose for which an individual did not intend it, and thus over which the individual no longer has control. The different levels of the "use of information" factor were operationalized in the vignettes as the person who is accessing the information sharing that information with (a) her mother (i.e., the personal context), (b) with a person in Human Resources (i.e., the professional context), and (c) entering that information in a direct mailing database (i.e., the business context). Subjects perception of a violation of privacy in the professional context was more likely than in the personal and business context, and in the professional context that violation was seen as most serious compared to the other conditions. In other words, entering information in a direct mailing database might be acceptable from a privacy perspective because it probably does not cause much harm, similar to sharing information in a personal context and thus might be perceived as less serious. However, using information obtained from Facebook in order to make decisions about hiring and promotion is potentially harmful to the individual and thus presumably considered more serious.

These differences in perceived privacy violation seriousness highlight the importance of not only examining the conceptions of privacy but also the underlying interests privacy is protecting and the potentially resulting harm from a privacy violation. In other words, without assessing the value of privacy in a given context, the picture we obtain by just assessing the occurrence of a privacy violation is incomplete. Particularly in a context in which privacy norms are in flux, distinguishing between violation and seriousness suggests the need for a more nuanced understanding of privacy. This was demonstrated by the work of Shadnam and Lawrence (2011) and Palazzo, Krings, and Hoffrage (2012) who proposed that ideological context was a significant factor affecting how

individuals present themselves and make ethical decisions in the workplace. In addition, we know from previous research that individuals sometimes give up information in order to receive some benefits from an interaction (Youn 2005). However, even in such situations the privacy expectations around the use of this information remain in place[2] (Metzger 2007; Nissenbaum 2004; Petronio 2002). In the Facebook context this could mean that individuals accept that Facebook might sell their information to third parties (who might then market products to the Facebook users) in exchange for being able to participate in the social network. However, there seems to be also a limit to how far the use of the information can go. Using information on Facebook to make decisions that can affect an individual's career do not seem to be acceptable.

While the majority of our hypotheses were supported by our data, some were not. Based on our data, the type of person accessing an individual's information did not affect privacy judgments (hypotheses 5 and 6). Possibly, the two privacy conceptions of dignity and liberty/freedom work in tandem and one aspect might become more dominant in some situations. In other words, the concern about control and what the information recipients do with the information they obtain might be more salient or important than the particular facet of one's identity that was supposed to be presented; thus we might not have found any differences in privacy judgments based on the person who accessed the information. Of course the lack of support for the hypotheses can also be due to the size of our sample, which precludes us from drawing further conclusions until the analyses are repeated using a larger pool of participants.

Our findings regarding hypotheses 3 and 4, which examined the influence of the type of information accessed on perceived privacy violation and seriousness, were also interesting. Drawing on the privacy as dignity concept, we assumed that access to information about social behavior (drinking at a party) and personal characteristics (vacationing with a same-sex partner) would be more of a privacy violation and more serious than access to information about purchasing behavior (buying an expensive necklace). However, we found the reverse. Access to personal information was *less* of a violation and less serious than access to social and purchase behavior. One possible reason for this unexpected result could be the way the factor was operationalized. The dominant concept of privacy that underpins the "type of information" factor might be control rather than dignity. In other words, the act of purchasing an expensive necklace, for example, could be interpreted in many different ways by the information recipient (being a shopaholic, being overly focused on appearance, etc.), which reduces the control the individual has over the information. On the

other hand, vacationing with a same sex partner is presumably a clear indication of the personal characteristics of the individual and thus there is less ambiguity and thus more control about what that information means. It is also possible that our operationalization conflated the purpose of Facebook with the type of information shared. After all, Facebook was initially designed around social and personal interaction, which presumably centers on personal information. For example, Facebook users can indicate relationship status and other personal characteristics about themselves very prominently. Therefore users might actually expect the personal information available on Facebook to be shared regarding their online personal self. Further investigation is needed to get a better understanding of how the type of information that is accessed influences privacy judgments and how it potentially interacts with the other privacy components, such as use of information.

Our results overall paint a much more nuanced picture of privacy perceptions in Facebook than is usually assumed both in the media as well as among businesses who increasingly use information from Facebook for a variety of purposes. The common narrative that in Facebook "anything goes" because presumably individuals have lower privacy expectations and put information about themselves into the "public" sphere does not seem to be quite accurate. The findings from our research indicate that there might in fact be some uses of Facebook that are legitimate (from a privacy perspective) but others that are not. For example, it might be acceptable to use one's own Facebook account to gather information about one's "friends" and use that information to develop new business. If individuals "like" corporations this business use of information about individuals seems to be relatively unproblematic. However, it would not be acceptable if a corporation uses someone else's account to receive access to information about current or prospective employees in order to make decisions about hiring or promotion. This supports the ethical perspective that individuals' privacy regarding what information they choose to share with different recipients must be maintained, at least on a personal level. A rights-based approach to this would consider not only the individual's right to choose, but also his or her right to privacy. Based on dignity as the conceptual basis for the need for privacy, it appears that an individual should have some right to choose the level at which his or her information is shared to protect his or her autonomy, identity, and dignity as a human being. In a business environment, however, the situation becomes more difficult.

If privacy can be conceptualized as control over information and protection of an individual's dignity, then corporations need to be much more cognizant of

the impact of their actions on the individual whose information is being sought. For example, requiring that prospective job applicants provide Facebook passwords might give applicants "control" over the information flow (e.g., they can remove items that they consider to be sensitive) but it undermines the control that the applicant's Facebook friends have over their information. Similarly, using Facebook to make decisions about hiring and promotion seems problematic in general. Not only can some information be interpreted in ways that Facebook users cannot control (e.g., did the picture of a person holding a bottle to their lips at a party really mean that this person is a "partier" and may be unreliable?) but it might also result in harm to the individual, which is why such uses might be considered serious privacy violations.

Consider, for example, the increasing number of corporations who are developing and using what are now called "identity management systems" (Kaupins, Coco, and Little 2012; Nuñez and Agudo 2014). These are systems and policies designed to gather and control personal information of employees. Casassa Mont and Thyne (2008) argue that "Privacy management is therefore important for enterprises: it has implications on their compliance with regulations, their reputation, brand and customers' satisfaction. Privacy policies can be used to represent privacy laws and guidelines: they describe people (data subjects)'s rights on their personal data, permissions given to enterprises and obligations that enterprises need to fulfil when handling personal data" (134).

Controlling information has become big business. What are the obligations of businesses to correctly handle individuals' personal, and potentially private, information? What are the obligations of the individuals to provide personal information to their employers? Corporations should be concerned with both the economic and ethical implications of such policies and systems. The identification of what individuals consider private versus public, or what information individuals are willing to share about their identities in various roles outside of the business context cannot be overlooked. Such policies need to be designed with the protection of individual privacy as a contextual concept that has far reaching implications. The fact that individuals behave in different ethical fashion outside of work has been extensively studied (see for example Gini 2011; Werhane 1999; Jackall 1988). What makes this challenging for determining the value of privacy today is the pervasiveness of social media as a significant (and growing) means of communication and human interaction.

Certainly the results of our study indicate the need for much more research before further conclusions can be drawn. For example, a larger number of subjects will allow for an analysis of the relative weights that subjects assign to the

various privacy factors. Furthermore, a follow-up study focusing on the privacy conceptualization as "freedom from harm" could yield more specific guidelines for privacy in the Facebook context in which privacy norms are still in flux and also overall different from areas outside of Facebook. We believe that our research helps to show that there continues to be a dichotomy between the person we are in the workplace and the person we are outside of the workplace, in terms of our desire to protect our identities and our dignity as well as to control information, in order to present a persona that is appropriate and acceptable for a professional role. This contrasts with the seemingly well-accepted idea that privacy does not necessarily exist in many ways in our culture as we go forward with the use of social media and the exchange of information on the Internet.

Facebook and social media are, and will continue to be, an integral part of human and business interactions going forward. How privacy violations are addressed within Facebook will likely shape how privacy is valued in our culture in the future. It is not a black and white concept and any successful means of protecting privacy in the digital age will require consideration of the many nuances of privacy and identity, both inside and outside Facebook.

Notes

1. In his overview Solove draws on the work of several researchers from various disciplines that have addressed the importance of privacy in personhood, intimacy, self-development, psychological functioning and nurturance of personal relationships (Altman 1975; Bloustein 1964; Fried 1970; Margulis 1977; Solove 2006; Strahilevitz 2005; Warren and Brandeis 1890; Westin 1967; Whitman 2004)

2. The recent Supreme Court ruling on Jones uses a similar notion of privacy—we regularly give information to others while maintaining privacy expectations around that information.

References

Abril, Patricia S. 2010. "Private Ordering: A Contractual Approach to Online Interpersonal Privacy." *Wake Forest Law Review* 45: 689–728.

Abril, Patricia S., Avner Levin, and Alissa Del Riego. 2012. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee." *American Business Law Journal* 49: 63–124.

Altman, Irvin. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding.* Monterey: Brooks/Cole.

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

Bloustein, Edward J. 1964. "Privacy as an Aspect of Human Dignity." *New York University Law Review* 39: 962–1007.

Bok, Sissela. 1983. *Secrets: On The Ethics of Concealment and Revelation*. New York: Panteon Books.

Bozeman, Dennis P., and K. Michele Kaemar. 1997. "A Cybernetic Model of Impression Management Processes in Organizations." *Organizational Behavior and Human Decision Processes* 69: 9–30.

Brandenburg, Carly. 2008. "The Newest Way To Screen Job Applicants: A Social Networker's Nightmare." *Federal Communications Law Journal* 60: 597–626.

Breckenridge, Adam C. 1970. *The Right to Privacy.* Lincoln: University of Nebraska Press.

Casassa Mont, Marco, and Robert Thyne. 2008. "Privacy Policy Enforcement in Enterprises With Identity Management Solutions." *Journal of Computer Security* 16: 133–163.

Christofides, Emily, Amy Muise, and Serge Desmarais. 2009. "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *Cyber Psychology and Behavior* 12: 341–345.

CNBC. 2012. "Social Media Use Gains Critical Mass Amongst Business Elite." Accessed October 24. http://www.cnbc.com/id/49530860/Social_Media_Use_Gains_Critical_Mass_Amongst_Business_Elite.

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

Electronic Privacy Information Center. 2013. "Facebook Privacy." Accessed May 21. http://epic.org/privacy/facebook.

Ellison, Nicole, Rebecca Heino, and Jennifer Gibbs. 2006. "Managing Impressions Online: Self-presentation Processes in the Online Dating Environment." *Journal of Computer-Mediated Communication* 11: 415–441.

Elzweig, Brian, and Donna K. Peeples. 2009. "Using Social Network Sites in Hiring and Retention Decisions." *SAM Advanced Management Journal* (Autumn): 27–35.

Etzioni, Amitai. 1999. *The Limits of Privacy.* New York: Basic Books.

Facebook. 2013. "Business Overview." Accessed March 24, 2013. https://www.facebook.com/business/overview.

Fried, Charles. 1970. *An Anatomy of Values: Problems of Personal and Social Choice*. Cambridge, MA: Harvard University Press.

Fusilier, Marcelline R., and Wayne D. Hoyer. 1980. "Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation." *Journal of Applied Psychology* 65: 623–626.

Gini, Al. 2011. "A Short Primer on Moral Courage." *In Moral Courage in Organizations: Doing the Right Thing at Work*, edited by Debra Comer and Gina Vega, 3–13. Armunk. New York: M.E. Sharpe.

Godkin, E. L. 1890. "The Rights of the Citizen, IV—To His Own Reputation." *Scribner's Magazine* (July–Dec.): 65.

Goffman, Erving. 1959 *The Presentation of Self in Everyday Life*. Garden City: Doubleday.

Herzog, Ari. 2012. "90% of Small Businesses Use Social Media." Accessed March 24, 2013. http://socialmediatoday.com/ariherzog/820046/90-percent-small-business-use-social-media

Hoadley, Christopher M., Heng Xu, Joey J. Lee, and Mary Beth Rosson. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry." *Electronic Commerce Research and Applications* 9: 50–60.

Jackall, Robert. 1988. *Moral Mazes: The World of Corporate Managers*. New York: Oxford University Press.

Jasso, Guillermina. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments." *Sociological Methods and Research* 34: 334–423.

Johnson. 1974. "Privacy as Personal Control." In *Man-environment Interactions: Evaluations and Applications*, edited by Daniel H. Carson, Part 2, Volume 6: 83–100.

Kaupins, Gundars, Malcolm Coco, and Andrew Little. 2012. "Organizational Social Networking Usage and Policy Restrictions." *International Journal of Business and Public Administration* 9: 38–54.

Kobsa, Alfred, Sameer Patil, and and Bertold Meyer. 2012. "Privacy in Instant Messaging: An Impression Management Model." *Behaviour and Information Technology* 31: 355–370.

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

LaPointe, Pat. 2012. "Measuring Facebook's Impact on Marketing." *Journal of Advertising Research* 52: 286–287

Levin, Avner, and Patricia S. Abril. 2009. "Two Notions of Privacy Online." *Vanderbilt Journal of Entertainment and Technology Law* 11: 1001–1051.

Liu, Yan, and Raymond Loi. 2012. "Ethical Leadership and Workplace Deviance: The Role of Moral Disengagement." In *Advances in Global Leadership* (Advances in Global Leadership, Volume 7), edited by William H. Mobley, Ying Wang, and Ming Li, 37–56. Emerald Group Publishing Limited.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15: 336–355.

Maltby, Emily, and Shira Ovide. 2013. "Small Firms Say LinkedIn Works, Twitter Doesn't." *Wall Street Journal*, Small Business, January 31, 2013.

Margulis, Stephen T. 1977. "Conceptions of Privacy: Current Status and Next Steps." *Journal of Social Issues* 33: 5–21.

Margulis, Stephen T. 1979. *Privacy as Information Management: A Social Psychological and Environmental Framework (NSBIR 79-1793)*. Washington: US Department of Commerce, National Bureau of Standards.

Margulis, Stephen T. 2003. "Privacy as a Social Issue and Behavioral Concept." *Journal of Social Issues* 59: 243–261.

Martin, Kirsten E. 2012. "Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract." *Journal of Business Ethics* 111(4): 519–539. DOI: 10.1007/s10551-012-1215-8.

Metzger, Miriam J. 2007. "Communication Privacy Management in Electronic Commerce." *Journal of Computer-Mediated Communication* 12: 335–361.

Miyazaki, Anthony D., and Ana Fernandez. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping." *Journal of Consumer Affairs* 35: 27–44.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 119–158.

Nock, Steven L., and Thomas Martin Gutterbock. 2010. "Survey Experiments." In *Handbook of Survey Research*, edited by James Wright and Peter Marsden. Bingley, UK: Emerald.

Nowak, Glen J., and Joseph Phelps. 1995. "Direct Marketing and the Use of Individual-level Consumer Information: Determining How and When 'Privacy' Matters." *Journal of Direct Marketing* 9: 46–60.

Nuñez, David, and Isaac Agudo. 2014. "BlindIdM: A Privacy-preserving Approach for Identity Management As a Service." *International Journal of Information Security* 13: 199–215.

Palazzo, Guido, Francisla Krings, and Ulrich Hoffrage. 2012. "Ethical Blindness." *Journal of Business Ethics* 109: 323–338.

Petronio, Sandra. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press.

Pollach, Irene. 2011. "Online Privacy as a Corporate Social Responsibility: An Empirical Study." *Business Ethics: A European Review* 20: 88–103.

Posner, Richard A. 1981. *The Economics of Justice*. Cambridge, MA: Harvard University Press.

Post, Robert C. 2001. "Three Concepts of Privacy." *The Georgetown Law Journal* 89: 2087–2098.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.

Reilly, A. 2012. "What Do Small Businesses Do on Social Media?" Accessed March 24, 2013. http://technorati.com/social-media/article/what-do-small-businesses-do-on.

Rosen, Jeffrey. 2000. *The Unwanted Gaze: The Destruction of Privacy in America.* New York: Random House.

Rossi, Peter H., and Steven L. Nock. 1982. *Measuring Social Judgments: The Factorial Survey Approach*. Beverly Hills, CA: Sage.

Shadnam, Masoud, and Thomas B. Lawrence. 2011. "Understanding Widespread Misconduct in Organizations: An Institutional Theory of Moral Collapse." *Business Ethics Quarterly* 21: 379–407.

Sheehan, Kim B., and Mariae G. Hoy. 2000. "Dimensions of Privacy Concern among Online Consumers." *Journal of Public Policy Marketing* 19: 62–73.

Shroff, Marie, and Annabel Fordham. 2010. "Do You Know Who I Am? Exploring Identity and Privacy." *Information Polity: The International Journal of Government and Democracy in the Information Age* 15: 299–307.

Singleton, Solveig. 1998. "Privacy as Censorship." *Cato Institute: Policy Analysis* No. 295.

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

Sprague, Robert. 2012. "Facebook Meets the NLRB: Employee Online Communications and Unfair Labor Practices." *University of Pennsylvania Journal of Business Law* 14: 957–1011

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154: 477–564.

Solove, Daniel. J. 2007. "'I've Got Nothing to Hide,' and Other Misunderstandings of Privacy." *San Diego Law Review* 44: 745–772.

Stein, Mari-Klara, Robert D. Galliers, and Lynne M. Markus. 2013. "Towards and Understanding of Identity and Technology in the Workplace." *Journal of Information Technology* 28: 167–182.

Stelzner, Michael A. 2012. "2012 Social Media Marketing Industry Report." *Social Media Examiner*, http://www.socialmediaexaminer.com/SocialMediaMarketingIndustryReport2012.pdf.

Strahilevitz, J. Lior. 2005. "A Social Networks Theory of Privacy." *University of Chicago Law Review* 72: 919–970.

Tan, Xin, Li Qin, Yongbeom Kim, and Jeffrey Hsu. 2012 "Impact of Privacy Concern in Social Networking Web Sites." *Internet Research* 22: 211–233.

Tufekci, Zeynep. 2008. "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites." *Bulletin of Science, Technology, and Society* 25: 20–36

Turkle, Sherry. 1995. *Life on the Screen: Identity in the Age of the Internet.* New York: Simon & Schuster.

Turkle, Sherry. 2011. *Alone Together*. New York: Basic Books.

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

Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193–220.

Werhane, Patricia. 1999. *Moral Imagination and Management Decision Making*. New York: Oxford University Press.

Westin, Alan F. 1967. *Privacy and Freedom.* New York: Athenarum.

Whitman, James Q. 2004. "The Two Western Cultures of Privacy: Dignity Versus Liberty." *Yale Law Journal* 113: 1151–1223.

Youn, Seounmi. 2005. "Teenagers' Perceptions of Online Privacy and Coping Behaviours: A Risk-Benefit Appraisal Approach." *Journal of Broadcasting and Electronic Media* 49: 86–110.