Article

new media & society
2018, Vol. 20(1) 50–67

DOI: 10.1177/1461444816654465
journals.sagepub.com/home/nms

Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors

Mary Helen Millham and David Atkin
University of Connecticut, USA

Abstract
Online social networks are designed to encourage disclosure while also having the ability to disrupt existing privacy boundaries. This study assesses those individuals who are the most active online: "Digital Natives." The specific focus includes participants' privacy beliefs; how valuable they believe their personal, private information to be; and what risks they perceive in terms of disclosing this information in a fairly anonymous online setting. A model incorporating these concepts was tested in the context of communication privacy management theory. Study findings suggest that attitudinal measures were stronger predictors of privacy behaviors than were social locators. In particular, support was found for a model positing that if an individual placed a higher premium on their personal, private information, they would then be less inclined to disclose such information while visiting online social networking sites.

Keywords
Communication privacy management theory, online social networks, personal information, privacy

Human beings are social animals whose "distinctive genius" involves their reliance on communication with each other (Bennett, 1967: 371). This innate desire to communicate with others often takes the form of disclosure; one chooses what and how much information to reveal to another (e.g. Derlega and Chaikin, 1977; Jourard, 1966; Lee, 2007; Palfrey

Corresponding author:
Mary Helen Millham, Department of Communication, University of Connecticut, Storrs, CT 06269-1259, USA.
Email: mary.millham@uconn.edu

and Gasser, 2008; Petronio, 1991, 2002; Wu et al., 2011; Zittrain, 2008). Such disclosure helps build community and human relationships, uniting disparate individuals through common and lasting connections (Levinson, 2013: 13).

While past communities might have congregated in public (Habermas, 1962 [1989]), more recently these community ties have been fostered in a more virtual space. Online social networks (OSNs) such as Facebook and Twitter have continued to increase in both popularity and influence (e.g. Stutzman et al., 2013; Zhang and Daugherty, 2009). Over time, these interactive, virtual communities have witnessed a significant convergence of information and communication among members (Burnett, 2000). In the decade since Facebook diffused from college campuses, Millennials (a.k.a. "digital natives")—those aged 18–33—remained the dominant demographic for OSN use (Zickuhr, 2010).

OSN posting norms—if not the enterprises themselves—often encourage the disclosure of an individual's personal, private information (PPI) (e.g. age, sexual or political orientation, birth date, social gatherings, purchases) (e.g. Clemens et al., 2015; Vitak, 2012; Vitak and Ellison, 2013). This type of disclosure is fraught with risk. Financial and professional risks might include identity theft, perhaps sanctions at work or school. As observers (e.g. Garfinkel, 2001; Palfrey and Gasser, 2008; Wu et al., 2011; Zittrain, 2008) suggest, as the popularity and usage of the Internet have increased, so have the risks to individual privacy and security. Based on the perception of risk and increased use of OSNs, it is important to examine how those individuals who value their PPI choose to disclose such information online.

Research suggests that posting messages on social media has a significant relationship with a desire for positive perception (Hunt et al., 2012; Krishnan and Atkin, 2014) and privacy-related behaviors (Vitak, 2012). Privacy management is reflected on social media sites connected to one's identity; therefore, these sites provide an important domain for inquiry. However, many social media users—particularly on a site such as Facebook—use their actual names, the kind of disclosure that we might logically expect to be inversely related to privacy concern. Thus, considering the emergence of OSNs, this study aims to examine the relationship between privacy variables among a millennial cohort that makes extensive use of these sites.

The aggregation of personal data onto computerized databases (Garfinkel, 2001; Margulis, 1977a; Zittrain, 2008) prompted a desire for the public to control "their" information (Margulis, 1977b; Regan, 1995). While there is agreement that individuals are concerned about privacy—and its loss—the disciplines cannot agree "on what privacy is or on whether privacy is a behavior, attitude, process, goal, phenomenal state or what" (Margulis, 1977a: 17). Indeed, the arrival of new online media has only further blurred these contextual influences (Wu et al., 2011; Zittrain, 2008). Research does, however, suggest that user attitudes and behaviors regarding their online disclosures and privacy evaluations exhibit a complex, interdependent relationship (Stutzman et al., 2012). This study assesses user conceptions of privacy among those individuals who have grown up with digital technologies and are the most active online: "Digital Natives" (Palfrey and Gasser, 2008). This is particularly true given their (a) heavy use of social media, which in turn provide (b) the most active forum through which users need to negotiate disclosures in light of privacy concerns. We focus, in particular, on user privacy beliefs, how

valuable they believe their PPI to be, and perceived risks of disclosing PPI in a largely anonymous online setting.

Current study

This study explicates a model governing privacy behavior in the context of OSN use among Millennials. In the following literature review, we consider privacy-related constructs within a larger model and how they can be measured, including existing evidence relating the constructs to each other. Positioning the various determinants of privacy behavior in the context of an integrated framework—particularly in light of finding generated by this technology savvy cohort—can help inform our understanding of privacy behaviors in emerging digital environments.

Past work has found that Facebook users with high privacy concerns tailor their disclosures on the site. Lampinen et al. (2009) found that privacy attitudes and behaviors play a critical role in whether individuals share content within a network. As Stutzman et al. (2012) note, privacy concerns are critical determinants of whether users exchange information on their network. They draw from Altman's (1975) seminal work when conceptualizing this as a fluid process, wherein individuals strategically control access to information about themselves by regulating their social interactions. Hogan (2010), for instance, notes that the increasing diversity of one's online network prompts some users to share only information that is appropriate for all of their connections (i.e. "the lowest common denominator" approach).

Stutzman et al. (2012) conclude that in order for their networks to respond appropriately, Facebook users need to disclose. Even so, "privacy concerns may serve as a barrier to some disclosures, especially if the resource request is more personal in nature …, and therefore the effects of privacy attitudes and behaviors on disclosures in [an OSN] are important to investigate" (Stutzman et al., 2012: 3). We can gain a better understanding of how this process unfolds in digital environments by reviewing key components of privacy.

Understanding privacy

Building on Altman's (1975) conception of privacy as an "*interpersonal boundary process*" (p. 6), Petronio (2002) developed a multilayered framework to her own disclosure studies. Petronio (1991, 2002) re-imagined her communication boundary management theory and renamed it the communication privacy management (CPM) theory. She further posited a self-protection regime, where individuals would control their interpersonal boundary by regulating how much private information they allowed to flow back and forth between others via "rules or criteria" (Petronio, 1991: 311).

One way to slow down the loss of privacy is by giving one more control over third party access to their own personal information (Austin, 2010). This implicates an inherent contradiction in social networks between the risks and benefits accompanying such disclosure. In their study of disclosure on Facebook, Stutzman et al. (2013) suggested that more detailed and granular privacy settings would lead to users feeling as if they

had a greater sense of control over their personal information and to whom they could disclose.

Petronio (1991) described the assumptions made about the risks involved in the dyadic act of both disclosing and receiving private information. The one who is revealing the information becomes vulnerable, while the receiver of said information may feel compelled to protect themselves, in turn (Petronio, 1991). As more people communicate through OSNs, the questions become (1) how much do people value their personal and private information? and (2) is disclosure of said information worth the risk? It is useful to consider that the valuation of a person's private information can provide motivation for increases or decreases in access, as use of motivation as a criterion for judging when (or whether) to disclose is an established tenet within the CPM theory. In order to provide a clearer understanding of this online disclosure dynamic, it is useful to explore conceptual elements of privacy.

Conceptualizing privacy

When an individual's personal information is situated in an electronic database, they fear a loss of control over how that information might be disseminated in the future. Palen and Dourish (2003) noted that, because information technologies have the ability to "disrupt or destabilize the regulation of boundaries," it is crucial to discuss the online aspects of privacy and boundary management (p. 131). One can then use Petronio's (1991) explanation of privacy management as a device that helps to balance an individual's identity with their social interactions when we explicate how one might choose to interact on an OSN.

People believe, for instance, they "own" their own PPI (Petronio, 2002). For the purposes of this study, the term "private" refers more to the information itself rather than the context within which it was disclosed.[1] When something is considered "private," the use and/or knowledge of that information is restricted. Building off of Bennett's (1967) description of the act of confession as a "revelation … of the most private secrets" (p. 373) to another individual, OSNs can be seen as a form of cyber-confessional. Working from the definitions of privacy and privacy management as boundary management (Altman, 1975, 1977; Petronio, 1991, 2002; Petronio and Durham, 2008), it is useful to examine how an individual's need for privacy might be affected by the level of disclosure. That is to say, is the type of information disclosed related to how much is disclosed and to whom it is disclosed? Petronio (2002) has defined privacy as a *necessary condition* which can be protected or given up via disclosure. Disclosure is a communication phenomenon; it is the act of telling. John (2013) describes disclosure on OSNs as "sharing," especially with regard to status updates—in these instances, "sharing is telling" (p. 175).

In the social media realm, where one's identity is highly prominent, privacy is a "critical" determinant of how and with whom users interact (e.g. Stutzman et al., 2012). Derlega and Chaikin (1977) defined self-disclosure as "what one person tells another about himself/herself" (p. 103). It follows, then, that disclosure of private information can be defined as revealing or sharing intimate knowledge about oneself to another. According to CPM theory, individuals manage their privacy and their boundaries in three

distinct ways: linkage, ownership, and permeability (Petronio, 2002). A key focus in this study involves the ways in which these three privacy management factors impact overall disclosure behavior. Based on these conceptual dynamics, we might expect that those who place a higher valuation on their PPI—particularly their perceived responsibility for owning and keeping it private—will be less likely to disclose on OSNs.

More formally, we hypothesize the following:

H1a. Valuation of personal information will decrease level of disclosure on OSNs.

H1b. Valuation of personal information will decrease perceived boundary connections for disclosure on OSNs.

H1c. Valuation of personal information will decrease perceived ownership of disclosure boundaries on OSNs.

H1d. Valuation of personal information will decrease perceived confidentiality of disclosure boundaries on OSNs.

Privacy has been discussed in terms of control, of being able to control the flow of information, especially information of an intensely personal, private nature (boyd, 2010). Previous studies have not necessarily conceptualized disclosure as a type of "flow control." But this can be a useful conceptualization, particularly when one thinks of disclosing in an online context where the individual has control of how much information others can see about themselves (and when), which we explore in turn.

Levels of disclosure. According to Petronio's (2004) timeline regarding the development of the CPM, there is an inherent "dialectical tension" any time an individual discloses private information, one that makes it "problematical" to consider disclosure without considering "a sense of privateness" at the same time (p. 196). Margulis (2003) noted how both revealing and concealing private information has the "potential for vulnerability" (p. 421). When individuals reveal their innermost private, private thoughts, they can open themselves up to "influence and possible exploitation" by others (Derlega and Chaikin, 1977: 109). Individuals must navigate a "range of privacy and disclosure" and determine just how much "privacy and publicness they wish to experience in any given interaction" (Petronio, 2002: 15). Ledbetter et al. (2011) examined attitudes and disclosure in the online context, specifically how online social connection interacts with self-disclosure and how that can predict communication on OSNs (i.e. Facebook). Stutzman et al. (2013) noted that disclosure and use of OSNs was often a simultaneous event.

Other studies have investigated more commercial aspects of disclosure via CPM within the context of e-commerce (Metzger, 2004, 2007), finding that individuals are more aware of risks when there are financial transactions involved. Such concerns over privacy can often lead to individuals providing false information as a means of protecting themselves (Metzger, 2004, 2007; Rainie et al., 2013). Recent research conducted by the Pew Internet & American Life Project showed that over 85% of individuals online have made some sort of effort to be "less visible online," with 18% faking their user name and 13% providing inaccurate information about themselves (Rainie et al., 2013: 4).

More recent studies have also found that contextual cues in commercial settings can play a role in perceptions of risk as well as what and how much is disclosed (John et al., 2011). Vitak and Ellison's (2013) study revealed that some users censored their disclosures on Facebook due to the risks of revealing information to a wide, sometimes unknown, audience. Child et al. (2009), for instance, expanded upon CPM with their findings that CPM's underlying concepts—outlined in the first set of hypotheses (boundary linkage, ownership, and permeability)—can influence one's blogging intentions. Based on that conception, we expect that one's level of perceived risk, ownership, and responsibility to protect private information will be inversely related to their willingness to disclose online. More formally,

H2a. Level of perceived risk associated with personal disclosure will decrease level of disclosure on OSNs.

H2b. Perceived risk associated with personal disclosure will decrease perceived boundary connections for disclosure on OSNs.

H2c. Perceived risk associated with personal disclosure on OSNs will decrease perceived ownership of disclosure boundaries on OSNs.

Taken together, we expect that the above privacy considerations will influence one's privacy valuations to varying degrees. It is useful to also consider other contexts for online disclosure, including blogs (Child and Agyeman-Budu, 2010; Child et al., 2009, 2011)and Facebook (Acquisti and Gross, 2006; Ledbetter et al., 2011; Vitak, 2012), which are explored in the section to follow.

Building a comprehensive theoretical framework for online privacy

CPM theory. Petronio (2002) conceptualized the theory as a "privacy management system" which was focused on the ways in which individuals coordinate their privacy boundaries between and among each other (p. 3). Petronio (2002) also described "the unity of opposites" in regard to CPM (p. 14). She argued that "privacy is a necessary condition," and, through the act of disclosure, an individual either protects this condition or abdicates it (p. 14). Disclosure is one of several concepts that help comprise theoretical notions about private information management. They can be summarized as a series of pairs that underscore the dialectical nature of private information management and privacy regulation: revealing versus concealment, disclosing versus protecting, granting versus denying access, and the like.

Researchers have indeed taken this interpersonal theory and applied it to a mediated, online environment and an individual's behavioral choices and attitudes in that environment (e.g. Vitak, 2012). Individuals tend to enact behaviors online that will minimize the ability of others to access their information, by modifying privacy settings (boyd and Hargittai, 2010; Stutzman et al., 2011), not disclosing personal identifiers, or disclosing false information (Culnan and Armstrong, 1999; Metzger, 2004, 2007; Metzger and Docter, 2003).

These sorts of filtering behaviors imply a lack of trust in others online. For instance, Mou et al. (2013) tested a "spiral of trust dynamic," one that explained higher levels of

trust driving online disclosure among trusted networks of friends. Based on these assumptions, it is logical to posit that trust in one's online discussion partners will positively influence perceptions of security and openness associated with disclosure. The final hypotheses to be tested on these various aspects of privacy management, then, are as follows:

H3a. Level of trust in others in one's online network will increase level of disclosure on OSNs.

H3b. Trust in others in one's online network will increase perceived boundary connections for disclosure on OSNs.

H3c. Trust in others in one's online network will increase perceived ownership of disclosure boundaries on OSNs.

H3d. Trust in others in one's online network will increase level of perceived confidentiality of disclosure boundaries on OSNs.

Methodology

Design

In order to ensure respondent confidentiality—given our focus on individual behaviors, attitudes, and concerns about disclosure and privacy in an online context—the survey was administered online. Because the study focus involved privacy in a new media environment, a sample of student "digital natives" (i.e. users who grew up with technology) (Palfrey and Gasser, 2008) was thought to be purposive as well as convenient (see boyd and Hargittai, 2010). The survey was hosted on QuestionPro, a site commonly used in social science research. Other than the descriptive and demographic questions, all other items were measured on a 7-point scale (1=*strongly disagree*, 7=*strongly agree*) for uniformity and to lessen range restriction.

Sample

All told, a total of 697 participants were recruited from a public university in the Eastern United States. A series of screening questions were asked to ensure that those taking the survey were active users of OSNs, leaving a total of 606 valid responses. We defined an "active user" as someone who logs onto an OSN at least once a day. In total, 83% of respondents were solidly in the "Millennial" or "digital native" demographic of 18- to 20-year old, 12% of respondents were 21-year old, and fewer than 5% of the respondents were between 23 and 26 years of age.

Measures

Disclosure. In order to operationalize the concept of disclosure on OSNs and build upon the foundations of CPM, the survey used a modified version of Child et al.'s (2009) blogging privacy management measure; full operationalizations of study measures are available

from the authors upon request. Child and Petronio (2011) have noted that modifications can be made to the language of the scale to reflect use of other forms of OSNs, rather than diary-based blogs, which is what their original scale measured.

Child et al. (2009) ran both exploratory and confirmatory factor analyses on their scale and divided it into three sub-measures (boundary permeability, boundary ownership, boundary linkage). They tested the resulting scale and its sub-measures through three different studies. The overall reliability of the full 18-item measure averaged out to be $\alpha = .76$. Child et al. found that Cronbach's alpha for each of the sub-measures averaged out over the three studies was $\alpha = .78$ for boundary permeability, $\alpha = .70$ for boundary ownership, and $\alpha = .72$ for boundary linkage.

For this study, in order to confirm that the sub-measures do reflect the factors described in Child et al.'s (2009) previous studies, a principal component analysis (PCA) was conducted on the 18 items with oblique rotation (oblimin). The Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy was .83 ("great," per Field, 2009), and all KMO values for individual items were >.63, which is above the acceptable limit of .5 (Field, 2009). Bartlett's test of sphericity was significant ($\chi^2(153) = 2403.199$, $p < .001$). The first component represents boundary linkage, that is, how people feel about connecting with others via social media. Component 2 concerns itself with boundary ownership or how much people look to control what is known about them in these online networks. The third component relates to boundary permeability or how comfortable people are with sharing information within an online setting.

Cronbach's alpha for the 18-item social networking privacy management scale in this study was $\alpha = .77$. Reliability tests were also run on the three 6-item sub-measures for boundary permeability ($\alpha = .78$), boundary ownership ($\alpha = .60$), and boundary linkage ($\alpha = .76$).

Child et al. (2009) scored their measure on a 7-point scale ranging from "never true" to "always true," with higher scores indicating more disclosures and less privacy or greater public access to information (2083). For the purposes of this study, the 18-item scale has been modified to replace the instances of the word "blog" with the phrase "social networking site(s)" or "social networking" and adding "groups" and "Facebook networks" to 1 item. The three factors of permeability, linkage, and ownership were transformed by averaging the scores for each factor (sub-measure). This larger variable, "disclosure," was formed by averaging the scores for the three sub-measures (permeability + ownership + linkage ÷ 3). The three sub-measures (permeability, ownership, linkage) were included in the multiple regression analyses to see which of the three factors, if any, had a greater effect on the other variables (PPI, risks, privacy beliefs, trust) than the full disclosure variable.

Online privacy concerns. To measure concerns about online privacy, the study operationalized the variables "premium of personal, private information" and "risk of disclosure" using scales originally combined by Yao et al. (2007). How people feel about the gathering of personal information by companies (organizational privacy) was measured by 13 items from Smith et al.'s (1996) original 15-item scale.

The other nine items used by Yao et al. (2007) concern "general online privacy" and were used with no modifications in this current study. All told, the 23 items used were

scored on a 7-point scale, ranging from "strongly disagree" (1) to "strongly agree" (7). Those items that pertain to perceptions of security were combined (scores averaged) into the "security" variable (α=.79), while those items that pertain to risks involved with disclosure were averaged into the "risks" variable (α=.84), and those items that are concerned with how valuable people perceive their information to be were averaged into the "PPI" variable (α=.88).

Privacy beliefs. The operationalization of privacy beliefs was done using Yao et al.'s (2007) belief in privacy rights scale. This was designed by Yao et al. in order to capture respondents' privacy rights beliefs and developed from "frequently cited definitions of privacy" (p. 716). In order to enhance the validity of this privacy beliefs measure, three additional items were added. To remain consistent with the other items in the questionnaire, this measure was also scored on a 7-point scale ("very strongly disagree" to "very strongly agree"). The final scale score was averaged as the "privacy beliefs" variable, and Cronbach's alpha for the expanded scale was α=.78.

Trust. To operationalize the trust variable, the study utilized 15 items from Rotter's (1967) 40-item Interpersonal Trust Scale, as cited in Chun and Cambell (1974). Items were removed from the original scale that were either not applicable in this context or whose wording was outdated. Rotter's (1967) study indicates that these are additive scales and the reliability α=.76. When reliability tests were run on the 15-item Trust scale, the resulting Cronbach's alpha was .61. Five of the 15 items were then removed from the scale, with the remaining elements producing a marginally acceptable reliability of α=.70.

The original scale was scored on a 5-point scale, ranging from 1 (*strongly agree*) to 5 (*strongly disagree*) (Chun and Cambell, 1974; Rotter, 1967); for consistency with all other measures, this was changed to 7-point scale with 1=strongly *disagree* and 7=strongly *agree*. As with the original, the scores were averaged for the scale to come up with the variable score for the "trust" variable. To test the four groups of hypotheses, multiple regressions were conducted in SPSS. Utilizing variables that have emerged as theoretically significant predictors in the literature, models regressed *age, sex*, and (1) *PPI*, (2) *risks of disclosure*, or (3) *trust* on dependent measures of (a) the *full disclosure boundary*, (b) *disclosure boundary linkage*, (c) *disclosure boundary ownership*, and (d) *perceived confidentiality of disclosure boundaries on OSNs*.

Results

Hypothesis testing

Hypotheses 1a, 1b, 1c, and 1d. The first group of hypotheses posited that if an individual placed a higher premium on their PPI, they would be less inclined to disclose such information while on OSNs. Four multiple regressions were run, using age and biological sex (0 if male; 1 if female) along with the PPI variable as the three independent variables in each model, using the enter method. Hypotheses 1b, 1c, and 1d examined how much the value of information affected the specific boundary factors within the disclosure variable (boundary linkage, boundary ownership, and boundary permeability). Inspection of

Table 1. Regression analysis of the effects of age, sex, and personal, private information (PPI) on the full disclosure boundary variable (Hypothesis 1a).

	B	*SE B*	β
Personal, private information	−.22	.03	−.30**
Sex (female)	−.14	.06	−.10*
Age	.01	.021	.01

SE: standard error.
$R^2 = .11$.
*$p < .05$; **$p < .001$.

Table 2. Regression analysis of the effects of age, sex, and personal, private information (PPI) on the disclosure boundary linkage variable (Hypothesis 1b).

	B	*SE B*	β
Personal, Private Information	−.26	.05	−.23**
Sex (female)	−.26	.10	−.12*
Age	.04	.04	.05

SE: standard error.
$R^2 = .08$.
*$p < .05$, **$p < .001$.

variance inflation factor (VIF) indicators revealed that multicollinearity was not a problem in any of the prediction models.

Across our analyses, the value that people place on their information was the most significant predictor of disclosure ($p < .001$); in other words, the more value one placed upon their PPI, the less likely they were to disclose that information within OSNs.

In particular, the first set of hypotheses posited that valuation of personal information will decrease (1) level of disclosure on OSNs (H1a), (2) perceived boundary connections for disclosure on OSNs (H1b), (3) perceived ownership of disclosure boundaries on OSNs (H1c), and (4) perceived confidentiality of disclosure boundaries on OSNs (H1d). Support was found for Hypotheses 1a, 1b, and 1c; those results are summarized in Tables 1 to 3. While Hypothesis 1d (not tabled) approached significance, it was not supported ($R^2 = .01$, adjusted $R^2 = .01$, $F(3, 527) = 2.576$, $p = .053$). The value that an individual placed upon their PPI, and their perception of how "private" this information was, did not affect how open or closed they were.

With regard to other elements within the regression models, age failed to emerge as a significant variable in any of our analyses. Biological sex was not a significant predictor of how permeable someone would let their disclosure boundary to be, but it was a significant predictor ($p < .05$) of overall disclosure ($\beta = -.10$), ownership of disclosure boundaries ($\beta = -.12$), and linkage of the disclosure boundaries ($\beta = -.12$).

Hypotheses 2a, 2b, and 2c. This next set of hypotheses predicted that an individual's perceptions of risk in disclosing their PPI on OSNs would negatively affect their decision to

Table 3. Regression analysis of the effects of age, sex, and personal, private information (PPI) on the disclosure boundary ownership factor (Hypothesis 1c).

	B	*SE B*	β
Personal, private Information	−.26	.04	−.30**
Sex (female)	−.19	.07	−.12*
Age	.01	.03	.01

SE: standard error.
$R^2 = .12$.
*$p < .05$; **$p < .001$.

Table 4. Regression analysis of the effects of age, sex, and risks of disclosure on the full disclosure boundary variable (Hypothesis 2a).

	B	*SE B*	β
Risks	−.08	.03	−.11*
Sex (female)	−.24	.23	−.26
Age	−.10	.08	−.32

SE: standard error.
$R^2 = .04$.
*$p < .05$.

Table 5. Regression analysis of the effects of age, sex, and risks of disclosure on the disclosure boundary linkage factor (Hypothesis 2b).

	B	*SE B*	β
Risks	.003	.05	.002
Sex (female)	−.38	.10	−.17**
Age	.03	.04	.04

SE: standard error.
$R^2 = .03$.
**$p < .001$.

disclose such information (see Tables 4 to 6). The risks variable was entered as one of the predictor variables in each of the multiple regressions, and the ascriptive variables of sex and age were entered as the other predictor variables.

Support was found for Hypotheses 2a and 2b; the more risks that someone perceived in disclosing information, the more ownership and responsibility they felt toward the information. The greater the connection that respondents had to the information, the less likely they would be to disclose sensitive information within an OSN. The most powerful relationships were found between biological sex, the perceived risks of disclosure, and the ownership one felt toward the information ($\beta_{Sex} = -.15$, $\beta_{Risks} = -.32$). The multiple regression model did not reveal any significant support for the idea that perception of

Table 6. Regression analysis of the effects of age, sex, and risks of disclosure on the disclosure boundary ownership factor (Hypothesis 2c).

	B	*SE B*	β
Risks	−.27	.03	−.32**
Sex (female)	−.24	.07	−.15**
Age	.01	.03	.012

SE: standard error.
$R^2 = .13$.
**$p < .001$.

risk would predict a greater belief in the sanctity of PPI (ns; $p = .611$). As above, age was not a significant predictor of disclosure.

Hypotheses 3a, 3b, 3c, and 3d. The final group of hypotheses posited that the level of trust an individual had in the relationship with others within their OSN would be positively related to the level of disclosure and the associated boundary management strategies (see Tables 7 to 9). Hypotheses 3a and 3b did receive support; trust predicted the level of disclosure ($\beta = -.21$), along with the linkage of the disclosure boundaries ($\beta = -.23$). The results for Hypothesis 3d (not tabled), which was concerned with boundary permeability management, approached significance but did not find support (ns; $p = .059$). With regard

Table 7. Regression analysis of the effects of age, sex, and trust on the full disclosure boundary variable (Hypothesis 3a).

	B	*SE B*	β
Trust	−.23	.05	−.21**
Sex (female)	−.19	.06	−.15*
Age	.002	.02	.004

SE: standard error.
$R^2 = .07$.
*$p < .05$; **$p < .001$.

Table 8. Regression analysis of the effects of age, sex, and trust on the disclosure boundary linkage factor (Hypothesis 3b).

	B	*SE B*	β
Trust	−.42	.08	−.23**
Sex (female)	−.33	.09	−.15*
Age	.02	.04	.02

SE: standard error.
$R^2 = .08$.
*$p < .05$; **$p < .001$.

Table 9. Regression analysis of the effects of age, sex, and trust on the disclosure boundary ownership factor (Hypothesis 3c).

	B	*SE B*	B
Trust	−.11	.06	−.08
Sex (female)	−.27	.07	−.17**
Age	.001	.03	.002

SE: standard error.
$R^2 = .04$.
**$p < .001$.

to the ascriptive variables, biological sex (female) was a significant predictor ($p < .05$) of overall disclosure ($\beta = -.15$), ownership of disclosure boundaries ($\beta = -.17$), and linkage of the disclosure boundaries ($\beta = -.15$). Age failed to emerge as a significant predictor in any of the prediction models for trust.

Discussion

This study set out to provide an empirical test of social disclosure influences on privacy disclosure behaviors amid a key demographic—Millennials (a.k.a. "digital natives")—presumed to be the most technologically literate, with a particular focus on daily OSN users. On balance, study results demonstrate that attitudinal measures derived from CPM theory were stronger predictors of privacy prediction behaviors than were social locators. When users are motivated by the level of valuation placed on private information, there is an impact on privacy rules and choices about revealing or concealing. Support was found for a model positing that individuals placing a higher premium on their PPI would, in turn, be less inclined to disclose such information while visiting OSNs.

These results confirm and extend past explorations of relationships between privacy attitudes and disclosure behaviors (e.g. Stutzman et al., 2013), particularly among those who place a greater value on their private information and feel protective of it. This finding is consistent with a raft of work addressing disclosure (e.g. Child and Agyeman-Budu, 2010; Child and Petronio, 2011; Child et al., 2011; Petronio, 1991, 2002; Rainie et al., 2013; Rosen, 2001). Importantly, our results support key elements of Petronio's (2007) CPM theory in an online environment; that is, users expressing a higher valuation for their PPI—particularly their perceived responsibility for owning and keeping it private—were less likely to disclose on OSNs.

The highly interactive design of websites currently encourages an unconscious oversharing of personal information (e.g. John, 2013; Zittrain, 2008), one about which users voice increasing concern (Vitak and Ellison, 2013; Wu et al., 2011). Yet paradoxically, the weakest relationship involved the concept of boundary permeability or access to what can be considered "secret" or private information. One possible explanation for this weak showing by the disclosure sub-measure could involve the very nature of OSNs, notably their permeability. These networks are designed to facilitate the sharing of information among users and there is an expectation (and presupposition) of mutual disclosure on such

sites. Users of OSNs may also view their disclosures on OSNs to be those that should not be considered private; that is, if a disclosure truly is private, it is unlikely to be disclosed via OSNs. Additionally, the nature of OSNs is that it comprises a network of "friends" whom one already trusts on some level.

In light of this dynamic, the positive linkage between trust and online disclosure seems logical and supports past work positing "trust spirals" in online environments (Mou et al., 2013). That is, as individuals gain trust in how their fellow users will handle their private information online, they might logically be more open about providing further postings. Of course, relational trust can be advanced through reciprocal disclosure. These findings could also be explained as a function of increased user trust in the privacy safeguards of social media, as Stutzman et al. (2011) found that such sites can mitigate concerns about disclosure by providing transparent privacy controls and policies.

The fact that females indicate higher levels of online trust is consistent with past work demonstrating that men and women indicate differing sets of needs where privacy is concerned (Child and Petronio, 2011). Past research has found gender differences, particularly with the disclosure of private information (Petronio and Martin, 1986) and with disclosure more generally (Dindia and Allen, 1992). Specifically, the greater interest shown by women in regulating disclosure is consistent with previous studies (e.g. Child and Petronio, 2011; Lewis et al., 2008; Petronio et al., 1984), which reported that women tend to regulate online disclosure more closely than do men. The fact that women are more trusting and yet more circumspect with their personal information may, on the surface, be paradoxical. But this dynamic may be a function of the fact that women choose to be more selective when engaging in online correspondences, but, when they do so, those tend to involve more trusting relationships.

The current results have implications for theory building, particularly in the OSN context, for CPM theory. Emulating Einstein's aphorism that there is nothing so practical as a good theory, Petronio (2007) notes that CPM theory has been "built to be *of* practice" so that it can "serve as a vehicle for research translation" (p. 218). Her goal has been to enable researchers who chose to use CPM theory to approach issues "such as privacy dilemmas, violations, and trust mistakes" (Petronio, 2007: 218). Practical implications stemming from the present findings suggest that OSNs (e.g. Facebook) could mitigate concerns about disclosure by clearly communicating enhanced privacy controls to users (Stutzman et al., 2011). Since its conception, several have applied and adapted CPM theory for online use (e.g. Child and Agyeman-Budu, 2010; Child et al., 2009, 2011; John et al., 2011; Ledbetter et al., 2011; Metzger, 2004, 2007; Metzger and Docter, 2003). To wit, the present findings underscoring a positive influence for trust on self-disclosure (e.g. involving purchase information) suggest that OSNs (e.g. Facebook) should extend their efforts to safeguard privacy within user networks.

The goal of this study is to render the findings on disclosure and privacy beliefs more generalizable to all OSNs, rather than one particular platform (e.g. a blog) or a single, specific site. To the limited extent that we could gauge its influence here, age had no effect on how much an individual would or would not disclose PPI within the context of an OSN. One potential explanation for this could involve the homogeneity of the sample, particularly in terms of age. While the ages ranged from 17 to 26, the majority of respondents were clustered in the 18- and 19-year-old groupings ($n = 194$ and 180, respectively).

Limitations

While this study utilized a non-randomized convenience sample, one benefit of such a participant pool is the fact that it can provide a picture of digital privacy attitudes among a technology-intensive cohort. The validity and reliability of some of the scales used (e.g. Yao et al.'s (2007) Privacy Beliefs Scale, Rotter's (1967) Trust Scale) could have been stronger, while the elimination of redundant items could help improve overall validity in later work. Future studies should continue to refine more valid and reliable scales, particularly as they apply to the sensitivities of the online environment. Another issue involves the inability to randomize the questions given to each participant while they were taking the survey online.

In sum, this study provides support for an original model on disclosure in an online environment. Such work can provide a foundation for later explorations that can enhance our understanding of the steps that users need to take in order to protect their privacy and their PPI. Later work should expand beyond the blog contexts explored here, since studies have shown that the use of that form of online discourse is declining, most noticeably among Millennials (Zickuhr, 2010). Instagram, Tumblr, SnapChat, and LiveJournal represent promising contexts for later work.

Recently, the Pew Research Center's Internet Project published results of a national survey (Rainie et al., 2013) documenting that the majority of Internet users—fully 55%—have made a specific effort to "hide from specific people or organizations" (Rainie et al., 2013: 5). The largest group (33%) that mask their digital profile want to "avoid being observed or seen by hackers or criminals," while only 5% reported they did not want to be found by the government (Rainie et al., 2013: 5). Issues surrounding online privacy are thus extremely timely and fluid, as the concept continues to evolve and is inter-disciplinary, allowing for multiple avenues of research. Longitudinal studies could be undertaken to allow researchers a chance to determine whether, and how, privacy beliefs and behaviors change over time and under what circumstances. Future research addressing online privacy behaviors can also examine how revelations about government surveillance and related current events have affected people's online behaviors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Note

1. Public information is that which is accessible to all members of the community; private information is that which can make one vulnerable if shared widely.

References

Acquisti A and Gross R (2006) Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Danezis G and Golle P (eds) *Privacy Enhancing Technologies: 6th International Workshop, PET 2006. Cambridge, UK, June 28-30, 2006, Revised Selected Papers*. Berlin: Springer, pp. 36–58.

Altman I (1975) *The Environment and Social Behavior: Privacy Personal Space Territory Crowding*. Monterey, CA: Brooks/Cole Publishing.

Altman I (1977) Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues* 33: 66–84.

Austin LM (2010) Control yourself, or at least your core self. *Bulletin of Science, Technology & Society* 30: 26–29.

Bennett CC (1967) What price privacy? *American Psychologist* 22: 371–376.

boyd d (2010) Making sense of privacy and publicity. Available at: http://www.danah.org/papers/talks/2010/SXSW2010.html

boyd d and Hargittai E (2010) Facebook privacy settings: who cares? Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/3086

Burnett G (2000) Information exchange in virtual communities: a typology. *Information Research* 5. Available at: http://informationr.net/ir/5-4/paper82.html (accessed 19 November 2009).

Child JT and Agyeman-Budu EA (2010) Blogging privacy management rule development: the impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior* 26: 957–963.

Child JT and Petronio S (2011) Unpacking the paradoxes of privacy in CMC relationships: the challenges of blogging and relational communication on the Internet. In: Wright KB and Webb LM (eds) *Computer-Mediated Communication in Personal Relationships*. New York: Peter Lang, pp. 21–40.

Child JT, Pearson JC and Petronio S (2009) Blogging, communication, and privacy management: development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology* 60: 2079–2094.

Child JT, Petronio S, Agyeman-Budu EA, et al. (2011) Blog scrubbing: exploring triggers that change privacy rules. *Computers in Human Behavior* 27: 2017–2027.

Chun K-T and Cambell JB (1974) Dimensionality of the Rotter interpersonal trust scale. *Psychological Reports* 35: 1059–1070.

Clemens C, Atkin D and Krishnan A (2015) The role of sexual orientation and personality traits on gratifications obtained through online dating websites. *Computers in Human Behavior* 49: 120–129.

Culnan MJ and Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science* 10: 104–115.

Derlega VJ and Chaikin AL (1977) Privacy and self-disclosure in social relationships. *Journal of Social Issues* 33: 102–115.

Dindia K and Allen M (1992) Sex differences in self-disclosure: a meta-analysis. *Psychological Bulletin* 112: 106–124.

Field A (2009) *Discovering Statistics Using SPSS*. Thousand Oaks, CA: SAGE.

Garfinkel S (2001) *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly Media.

Habermas J (1962 [1989]) *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MA: The MIT Press.

Hogan B (2010) The presentation of self in the age of social media: distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society* 30: 377–386.

Hunt D, Atkin D and Krishnan A (2012) The influence of computer-mediated communication apprehension on motives for Facebook use. *Journal of Broadcasting & Electronic Media* 56: 187–202.

John LK, Acquisti A and Loewenstein G (2011) Strangers on a plane: context-dependent willingness to divulge sensitive information. *Journal of Consumer Research* 37: 858–873.

John NA (2013) Sharing and web 2.0: the emergence of a keyword. *New Media & Society* 15: 167–182.

Jourard SM (1966) Some psychological aspects of privacy. *Law and Contemporary Problems* 31: 307–318.

Krishnan A and Atkin D (2014) Individual differences in social networking site users: the interplay between antecedent variables and the subsequent effect on level of activity. *Computers in Human Behavior* 30: 111–118.

Lampinen A, Tamminen S and Oulasvirta A (2009) "All my people right here, right now": management of group co-presence on a social networking site. In: *Proceedings of the ACM 2009 international conference on supporting group work,* Sanibel Island, FL, 10–13 May.

Ledbetter AM, Mazer JP, DeGroot JM, et al. (2011) Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness. *Communication Research* 38: 27–53.

Lee LT (2007) *Digital Media Technology and Individual Privacy: Communication Technology and Social Change*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 257–279.

Levinson P (2013) *New New Media*. Upper Saddle River, NJ: Pearson.

Lewis K, Kaufman J and Christakis N (2008) The taste for privacy: an analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication* 14: 79–100.

Margulis ST (1977a) Conceptions of privacy: current status and next steps. *Journal of Social Issues* 33: 5–21.

Margulis ST (1977b) Introduction. *Journal of Social Issues* 33: 1–4.

Margulis ST (2003) On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59: 411–429.

Metzger MJ (2004) Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* 9: 00. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2004.tb00292.x/abstract

Metzger MJ (2007) Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 12: 1–27.

Metzger MJ and Docter S (2003) Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting & Electronic Media* 47: 350–374.

Mou Y, Atkin D, Fu H, et al. (2013) The influence of online forum and SNS use on online political discussion in China: assessing "Spirals of Trust". *Telematics and Informatics* 30: 359–369.

Palen L and Dourish P (2003) Unpacking "Privacy" for a networked world. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Fort Lauderdale, FL, 5–10 April, pp. 129–136. New York: ACM.

Palfrey J and Gasser U (2008) *Born Digital: Understanding the First Generation of Digital Natives*. New York: Basic Books.

Petronio S (1991) Communication boundary management: a theoretical model of managing disclosure of private information between marital couples. *Communication Theory* 1: 311–335.

Petronio S (2002) Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication* 4: 193-207.

Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.

Petronio S (2007) Translational research endeavors and the practices of communication privacy management. *Journal of Applied Communication Research* 35: 218–222.

Petronio S and Durham WT (2008) Communication privacy management theory. In: Baxter LA and Braithwaite DO (eds) *Engaging Theories in Interpersonal Communication: Multiple Perspectives*. Los Angeles, CA: SAGE, pp. 309–322.

Petronio S and Martin JN (1986) Ramifications of revealing private information: a gender gap. *Journal of Clinical Psychology* 42: 499–506.

Petronio S, Martin J and Littlefield R (1984) Prerequisite conditions for self-disclosing: a gender issue. *Communication Monographs* 51: 268–273.

Rainie L, Kiesler S, Kang R, et al. (2013) Anonymity, privacy, and security online. *Pew Research Center's Internet & American Life Project*, 5 September. Available at: http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Regan PM (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: The University of North Carolina Press.

Rosen J (2001) *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage Books.

Rotter JB (1967) A new scale for the measurement of interpersonal trust. *Journal of Personality* 35: 651–665.

Smith HJ, Milberg SJ and Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* 20: 167–196.

Stutzman F, Capra R and Thompson J (2011) Factors mediating disclosure in social network sites. *Computers in Human Behavior* 27: 590–598.

Stutzman F, Gross R and Acquisti A (2013) Silent listeners: the evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality* 4: 7–41.

Stutzman F, Vitak J, Ellison NB, et al. (2012) Privacy in interaction: exploring disclosure and social capital in Facebook. In: *Proceedings of the sixth international AAAI conference on web and social media.* Washington, DC: Association for the Advancement of Artificial Intelligence, pp. 330-337.

Vitak J (2012) The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* 56: 451–470.

Vitak J and Ellison NB (2013) "There's a network out there you might as well tap": exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media & Society* 15: 243–259.

Wu Y, Lau TY, Atkin D, et al. (2011) A comparative study of online privacy regulations in the U.S. and China. *Telecommunications Policy* 35: 603–616.

Yao MZ, Rice RE and Wallis K (2007) Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology* 58: 710–722.

Zhang J and Daugherty T (2009) Third-person effect and social networking: implications for online marketing and word-of-mouth communication. *American Journal of Business* 24: 53–63.

Zickuhr K (2010) Generations 2010. *Pew Internet & American Life Project*, 16 December. Available at: http://www.pewinternet.org/2010/12/16/generations-2010/

Zittrain J (2008) *The Future of the Internet and How to Stop It*. New Haven, CT: Yale University Press.

Author biographies

Mary Helen Millham (MA, University of Hartford) is a doctoral student at the University of Connecticut whose research interests include privacy behaviors and how these behaviors pertain to social media and mobile applications, the mass media, and new media technologies.

David Atkin (PhD, Michigan State University) is a professor of Communication at the University of Connecticut. His research interests include communication policy as well as the uses and effects of new media.