



Article

Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users

new media & society

2018, Vol. 20(1) 141–161

© The Author(s) 2016

Reprints and permissions:

sagepub.co.uk/journalsPermissions.nav

DOI: 10.1177/1461444816660731

journals.sagepub.com/home/nms



Mina Tsay-Vogel

Boston University, USA

James Shanahan

Indiana University, USA

Nancy Signorielli

University of Delaware, USA

Abstract

In light of the omnipresence of personal information exchange in the virtual world, this study examines the effects of Facebook use on privacy perceptions and self-disclosure behaviors across a 5-year period from 2010 to 2015. Findings at the global level support the socializing role of Facebook in cultivating more relaxed privacy attitudes, subsequently increasing self-disclosure in both offline and online contexts. However, longitudinal trends indicate that while risk perceptions increased for heavy users, they remained stable for light users. Furthermore, the negative relationship between privacy concerns and self-disclosure weakened across time. Implications for the application of cultivation theory to a contemporary social media context and the year-to-year changes in the impact of Facebook use on privacy attitudes and self-disclosure are discussed.

Keywords

Cultivation, Facebook, privacy, self-disclosure, social networking

Corresponding author:

Mina Tsay-Vogel, Department of Mass Communication, Advertising & Public Relations, Boston University, 640 Commonwealth Avenue, Boston, MA 02215, USA.

Email: minatv@bu.edu

In today's rapidly evolving digital age, the exchange of personal information in the virtual world is ubiquitous. With the influx of social networking sites (SNSs) that encourage users to create personal profiles and networks with close and distant others (boyd and Ellison, 2007), self-disclosure now seems to be perceived as essential for the development and maintenance of relationships (Nosko et al., 2010). Specifically, updating profile information, posting status updates, sharing photos and videos, and commenting on others' posts—to name a few—are behaviors that reveal aspects of one's personal identity. However, this escalating personal exchange on SNSs also raises questions about privacy risks and consequences (Fogel and Nehmad, 2009). Research shows that factors such as attitudes toward privacy, security, and transparency can impact online disclosure practices (Acquisti and Gross, 2006).

In light of the pervasive revelation of personal information on SNSs, the theme of *self-disclosure* is distinctly prevalent in the social media landscape. Being immersed in a virtual environment where personal information (e.g. names, addresses, opinions, and values) is easily shared may have implications for more relaxed privacy boundary management, perhaps leading users to see the world as less regulated by privacy concerns. This study uniquely applies a cultivation perspective to examine the effects of SNSs on privacy attitudes and self-disclosure behaviors. Initially established in the context of television (Gerbner, 1969), cultivation theory suggests that heavy viewing of similar messages or storytelling elements across television programs *cultivates* conceptions of reality (Gerbner et al., 1994). Specifically, heavy viewers are more likely to perceive the world in ways that closely mirror reality as portrayed on television. Given the theoretical assumptions of cultivation, SNSs may also serve as socializing agents for users (Morgan et al., 2015), particularly by representing a mediated reality inundated with the disclosure of personal information. This application of a traditional media effects theory to a contemporary context can provide invaluable insight into the potential long-term effects of SNSs on users' attitudes toward privacy and estimated risks of self-expression.

As Facebook's (2016) immense popularity draws more than 1 billion active users, this research uses it as a relevant SNS context to investigate whether exposure to repetitive themes of self-disclosure on Facebook cultivates weaker perceived threats to privacy, in turn, leading to greater self-disclosure. To test these relationships, longitudinal data in a 5-year period from 2010 to 2015 were collected to assess trends in Facebook use, privacy perceptions (i.e. threat to general privacy, threat to online privacy, and support for governmental privacy protection), and offline and online self-disclosure. Examination of these trends not only contributes to our understanding of the cognitive and behavioral effects of social media use associated with information exchange in recent years, but it also identifies meaningful patterns in the impact of SNS usage on privacy perceptions and self-disclosure behaviors in the future.

Omnipresence of self-disclosure on SNSs: a cultivation perspective

Self-disclosure refers to communication behavior in which an individual consciously makes himself or herself known to others (Derlega and Berg, 1987). SNSs offer many tools and features that by default foster self-disclosure among users (Nguyen et al.,

2012). In fact, social capital researchers suggest that people must be willing to reveal personal information in order to fully experience the relational benefits of social media use (Vitak, 2012). Because the non-verbal cues (e.g. eye contact and physical proximity) and social cues (e.g. indicators of certainty and confidence) that are commonly available in face-to-face (FTF) interactions are non-existent in computer-mediated communication (CMC) (High and Caplan, 2009), greater depth and breadth of self-disclosure are needed to compensate for the absence of these cues (Gibbs et al., 2011). CMC researchers have found that self-disclosure not only helps to initiate social interactions, but also facilitates richer social contacts and friendships in the long-term (Nosko et al., 2010).

Taking into account the omnipresence of self-disclosure on SNSs, it is reasonable to suggest that prolonged exposure to conventional practices of personal information exchange can impact perceptions associated with disclosure practices. Cultivation theory suggests a meaningful hypothesized link between exposure to common message themes and social reality perceptions. The theory postulates that television programs share comparable storytelling elements, and that heavy exposure to these universal and homogeneous themes cultivate similar conceptions of reality for viewers (Gerbner et al., 1994). Consequently, heavier viewers will have a greater tendency to perceive the world in ways that parallel representations of reality on television. Whereas cultivation research initially focused on television violence, showing evidence that heavy television exposure is related to inflated perceptions of crime (Shanahan and Morgan, 1999), cultivation effects have also been documented in the areas of gender roles (Signorielli and Lears, 1992), science (Dudo et al., 2011), and affluence (Shrum et al., 1998), among others. Although cultivation studies have traditionally concentrated on television as the message system, the theory may also be relevant to SNSs as a collective symbolic environment conveying shared stories and values (Morgan et al., 2015). On SNSs, the boundaries of content may potentially be expanded to include the activities that users commonly witness in online forums as these visible behaviors can also implicitly serve as storytelling elements characteristic of the social media system. Persistent exposure to such user behaviors may in turn cultivate one's world view. For instance, social media users are consistently exposed to mediated forms of self-disclosure, and this prevailing theme of personal information exchange can have a cumulative impact on one's social reality, particularly perceptions related to the domain of privacy. The application of cultivation theory to social media not only brings to light the notion of content that resides outside of tangible message features, but also theoretically points to the idea that observable activities in an environment can also be part of the overall message system attributed to newer media.

With a deluge of personal information available on SNSs, issues related to privacy have generated extensive attention (Spencer, 2002). Privacy precaution has been attributed to the impact of digital technologies on breaking down spatial distances, thus making communication barriers more permeable. However, as SNSs serve as platforms where the revelation of personal information is encouraged and minimal privacy settings are employed (Acquisti and Gross, 2006; Davis and James, 2012; Debatin et al., 2009), privacy boundaries among users may progressively become more relaxed. This prediction is informed by taking a cultivation perspective when considering the prevalence of self-disclosure on SNSs. Given the considerable amount of information exchange that

occurs in the virtual environment, it is reasonable to suggest that social media are cultivating more lenient privacy attitudes and beliefs as a result of the visible omnipresence of online self-disclosure activities in which users commonly, habitually, and intentionally engage. In a similar vein, research in the area of information privacy also focuses on people's attitudes toward safeguarding their privacy at an institutional level as threats to privacy are largely associated with the desire for privacy protection (Lyon and Zureik, 1996). In light of the inundation of personal data revealed in the virtual world, the abundance of information that is freely and publicly shared by users is likely to promote a culture where both perceived threat to privacy and support for privacy protection are mitigated. Therefore, the following hypothesis is posited:

H1. Facebook use is associated with privacy perceptions, specifically decreased (a) threat to general privacy, (b) threat to online privacy, and (c) support for governmental privacy protection.

Privacy attitudes predicting self-disclosure

The second focus of this research is driven by the association between attitudes and behaviors. In particular, the relationship between privacy attitudes and self-disclosure behaviors has largely been explained by the notion that individuals regulate their exchange of information based on privacy control mechanisms (Altman, 1975; Petronio, 2002). Disclosure is not only the core process through which relational satisfaction and maintenance are attained, but also one that is consistently adjusted in relation to one's privacy attitudes, goals, and knowledge. The concept of privacy as boundary regulation also considers how individuals draw on these domains when constructing self- and dyadic privacy strategies for disclosure (Derlega and Chaikin, 1977). Therefore, environmental assessments (e.g. perceived risk, safety, and transparency) play a role in shaping the propensity for people to freely share information. Recent work has corroborated the pivotal role of privacy attitudes in guiding disclosure behaviors in the context of SNSs (Stutzman et al., 2011; Vitak and Ellison, 2013).

In a similar vein, the theory of reasoned action (TRA) (Fishbein and Ajzen, 1975) provides another explanation for the attitude-behavior link, proposing that behavioral intention is a product of one's relevant attitudes and beliefs. Applying the assumptions of TRA to the issue of privacy, one might predict that those who hold more relaxed views of privacy have stronger intentions to self-disclose. In other words, attitudes associated with reduced privacy risks and concerns could subsequently lead to greater information sharing on SNSs.

Although SNSs offer users the opportunity to enrich their social interactions in a virtual space, research has supported the overlap between online and offline networks (Subrahmanyam et al., 2008). In particular, many people rely on their online communication behaviors to strengthen their offline connections, suggesting that online and offline disclosures and their relational benefits are symbiotic in nature. Therefore, privacy attitudes have the potential to impact self-disclosure behaviors in both synchronous and asynchronous domains. Although social information processing (SIP) theory (Walther, 1996) posits that self-disclosure is more frequent in the CMC, as compared to

FTE, context due to the compensation for loss of cues in a less media rich environment, there is inconsistent evidence of which setting fosters greater self-disclosure (Nguyen et al., 2012). Hence, due to the psychological interrelationships between online and offline interpersonal exchange (Lampe et al., 2007), this study also expects that privacy attitudes will impact offline and online disclosure practices similarly. Therefore, the next set of hypotheses is drawn:

H2. Privacy perceptions, specifically (a) threat to general privacy, (b) threat to online privacy, and (c) support for governmental privacy protection, are negatively associated with offline self-disclosure.

H3: Privacy perceptions, specifically (a) threat to general privacy, (b) threat to online privacy, and (c) support for governmental privacy protection, are negatively associated with online self-disclosure.

Trends in privacy perceptions and self-disclosure

The third direction of this research takes into consideration the element of time. As SNSs have become successfully diffused in society—74% of online adults use SNSs, 71% of online adults use Facebook, and the heaviest users of SNSs are between 18 and 29 years of age (Pew Research Center, 2014)—what are the trends in privacy perceptions and self-disclosure behaviors in recent years?

Whereas the dissemination of large quantities of personal information in the virtual environment has elevated concerns over privacy (Fogel and Nehmad, 2009), the body of research on privacy threats, security, and regulation shows mixed results. On the one hand, scholars point to the negative implications of the disclosure of personal data as it is related to identity theft, harassment, cyberstalking, bullying, and unwarranted rumors and gossip (Tavani and Grodzinsky, 2002). On the other hand, although users report being aware of privacy risks, they do little to implement safeguards to protect their personal information (Dwyer et al., 2007). Debatin et al. (2009) found that despite Facebook users reporting high familiarity with privacy settings, they readily accept acquaintances and strangers as “friends.” Given these discrepant patterns of privacy perceptions and self-disclosure behaviors, we inquire about the nature of these trends during the previous 5 years. Therefore, the following research questions are posed:

RQ1. Are there significant changes in privacy perceptions, specifically (a) threat to general privacy, (b) threat to online privacy, and (c) support for governmental privacy protection, in the time frame between 2010 and 2015?

RQ2. Are there significant changes in offline and online self-disclosure in the time frame between 2010 and 2015?

Considering the diversification of social media, growing accessibility of SNSs on mobile devices (e.g. cell phones, tablets, and watches), and increasing levels of personal information exchange in today’s virtual climate, it is also possible that the relationships between (1) SNS use and perceptions of privacy as proposed in H1 and (2) perceptions

of privacy and frequency of self-disclosure as proposed in H2 and H3 vary from year to year. Whereas prior research examining these associations has relied primarily on cross-sectional data, the current study offers a more comprehensive look into social media's impact on privacy attitudes and disclosure behaviors through a longitudinal trend analysis across 5 years. The potential interaction effects of these variables with time can not only elucidate our understanding of the long-term changes in SNSs' impact on users' perspectives of privacy and self-disclosure practices, but also allow us to forecast patterns in the upcoming years. Hence, the following research questions are addressed:

RQ3. Do the relationships between Facebook use and privacy perceptions, specifically (a) threat to general privacy, (b) threat to online privacy, and (c) support for governmental privacy protection, differ in the time frame between 2010 and 2015?

RQ4. Do the relationships between privacy perceptions and (a) offline disclosure and (b) online disclosure differ in the time frame between 2010 and 2015?

Method

Participants and procedure

This study employed a longitudinal design to test the three hypotheses and address the four research questions. The design features a trend study that drew on samples of different respondents from the same population at different time points. Specifically, a web-based questionnaire was administered annually between March and May during a 5-year period from 2010 to 2015. Data were collected using the same questionnaire across the consecutive years from undergraduate students in equivalent introductory communication classes at two large universities in the northeast region of the United States.

This longitudinal study captured a total of 2789 respondents (2010: $n=434$; 2011: $n=440$; 2012: $n=556$; 2013: $n=428$; 2014: $n=452$; 2015: $n=479$). Participants ranged in age from 18 to 25 years ($M=19.47$, standard deviation [SD]=1.29) with 28.2% males and 71.0% females. The racial composition of the sample was 6.2% African American, 0.5% American Indian, 9.7% Asian or Pacific Islander, 78.6% Caucasian, 8.4% Hispanic, and 5.4% other. The questionnaire consisted of items measuring respondents' Facebook use, privacy perceptions, and self-disclosure behaviors, followed by demographic questions.

Measures

Facebook use. Adapting Shrum et al.'s (1998) procedures to the context of Facebook, participants were asked to report the number of hours and minutes they consume Facebook during an average weekday and average day during the weekend in the morning, afternoon, evening, and late night periods. These data were combined (weighting the average weekday questions by a factor of five compared to the average day during the weekend by a factor of two) to construct a measure of Facebook use in hours per day during a regular week. Participants reported an average of 3.17 hours per day ($SD=1.32$) of Facebook use. Across the 5-year period, an analysis of variance shows statistically significant decreases in Facebook use from year to year, $F(5, 2714)=15.01$, $p<.001$

(2010: $M=4.25$, $SD=1.50$; 2011: $M=3.78$, $SD=1.28$; 2012: $M=3.42$, $SD=1.44$; 2013: $M=2.94$, $SD=1.47$; 2014: $M=2.53$, $SD=1.54$; 2015: $M=2.20$, $SD=1.21$).

Privacy perceptions. Three distinct dimensions of perceptions of privacy were assessed using 7-point Likert scales ranging from 1 (*strongly disagree*) to 7 (*strongly agree*): threat to general privacy, threat to online privacy, and support for governmental privacy protection.

Threat to general privacy. Eight items were used to assess an individuals' attitude toward privacy in general. Items were adapted from information privacy measures by Smith et al. (1996) and Stone et al. (1983) that tapped into attitudes pertaining to the caution and risks associated with the disclosure of personal information. Example items include the following: *People should be cautious about disclosing personal information to others*, *The idea that information about me is public makes me feel personally in danger*, and *People should pay less attention to safeguarding their privacy* (reverse-coded) (Cronbach's $\alpha=.83$; $M=4.84$, $SD=0.75$).

Threat to online privacy. To measure respondents' perceived threat to privacy on the Internet, a 10-item scale was adapted from Smith et al.'s (1996) information privacy scale that tapped into attitudes related to privacy dangers in the virtual environment. Example items include the following: *The Internet causes serious privacy problems*, *I am cautious of trusting people online*, and *The idea of someone stealing my identity online worries me* (Cronbach's $\alpha=.90$; $M=5.11$, $SD=0.70$).

Support for governmental privacy protection. Three items were adapted from Smith et al.'s (1996) information privacy scale that measured individuals' attitude in favor of governmental intervention that protects people's privacy, as well as their concern about improper access to personal information. The items include the following: *The government should take more steps to make sure that unauthorized people cannot access personal information in their computers*, *Computer databases that contain personal information should be protected from unauthorized access*, and *The government should put more effort into preventing unauthorized access to personal information online* (Cronbach's $\alpha=.79$; $M=4.76$, $SD=0.90$).

Self-disclosure. Two types of self-disclosure behaviors were assessed using 7-point Likert scales ranging from 1 (*not at all*) to 7 (*very much*): offline and online self-disclosure.

Offline self-disclosure. To measure the degree to which participants disclose personal information in FTF conversations, they were asked to rate the following statements: *I freely share my personal information with others face-to-face*, *I do not share personal information with others in conversation* (reverse-coded), and *I disclose information about myself to others in person* (Cronbach's $\alpha=.87$; $M=4.21$, $SD=1.12$).

Online self-disclosure. Three items were used to assess the extent to which participants reveal personal information to others on the Internet. These statements include the

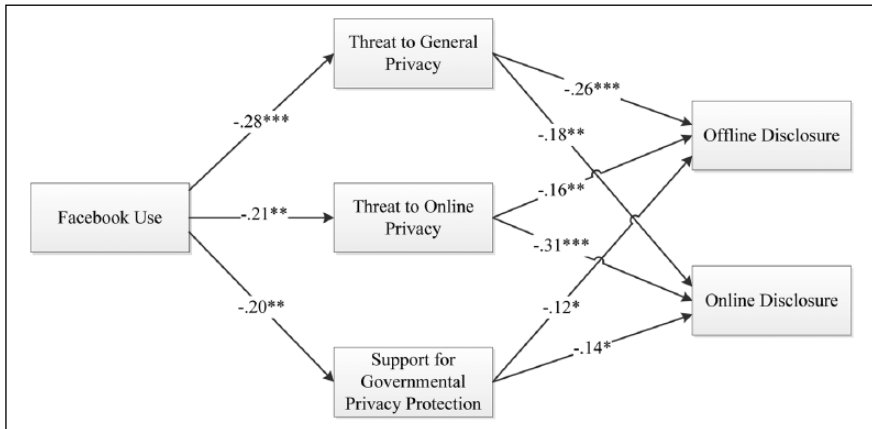


Figure 1. Path analysis of relationships among Facebook use, privacy perceptions, and self-disclosure, $\chi^2(6) = 5.15$, $p = .31$, CFI = 1.0, RMSEA = .05.

CFI: comparative fit index; RMSEA: root mean square error of approximation.

* $p < .05$; ** $p < .01$; *** $p < .001$.

following: *I freely share my personal information with others online*, *I do not share personal information with others on the Internet* (reverse-coded), and *I disclose information about myself to others online* (Cronbach's $\alpha = .89$; $M = 3.92$, $SD = 0.77$).

Results

Hypothesis tests

To test the three hypotheses, a path analysis was employed to determine if Facebook use predicted privacy perceptions, particularly threat to general privacy, threat to online privacy, and support for governmental privacy protection (H1). Subsequently, we examined if these three privacy perception domains were associated with offline disclosure (H2) and online disclosure (H3), respectively. The model (see Figure 1) was tested using AMOS and yielded an acceptable fit, $\chi^2(6) = 5.15$, $p = .31$, comparative fit index (CFI) = 1.0, root mean square error of approximation (RMSEA) = .05.

Consistent with our hypotheses, Facebook use was associated with decreased threat to general privacy ($\beta = -.28$, $p < .001$), threat to online privacy ($\beta = -.21$, $p < .01$), and support for governmental privacy protection ($\beta = -.20$, $p < .01$). In turn, less threat to general privacy, threat to online privacy, and support for governmental privacy protection were associated with increased offline disclosure ($\beta = -.26$, $p < .001$; $\beta = -.16$, $p < .01$; $\beta = -.12$, $p < .05$) and online disclosure ($\beta = -.18$, $p < .01$; $\beta = -.31$, $p < .001$; $\beta = -.14$, $p < .05$), respectively.

Bootstrapping procedures using 2000 bootstrap samples and bias-corrected confidence intervals revealed that privacy perceptions played significant mediating roles. Specifically, threat to general privacy ($\beta = -.28$, $p < .001$), threat to online privacy ($\beta = -.19$, $p < .01$), and support for governmental privacy protection ($\beta = -.14$, $p < .05$)

Table 1. Trends in privacy perceptions between 2010 and 2015.

Privacy perceptions		Year					
		2010	2011	2012	2013	2014	2015
Threat to general privacy	<i>M</i>	4.68 _a	4.78 _{ab}	4.79 _{ab}	4.91 _{ab}	4.92 _b	4.94 _b
	<i>SD</i>	0.87	0.80	0.78	0.72	0.70	0.71
Threat to online privacy	<i>M</i>	4.98 _a	5.05 _{ab}	5.07 _{ab}	5.12 _{ab}	5.17 _b	5.19 _b
	<i>SD</i>	0.81	0.79	0.68	0.65	0.72	0.67
Support for governmental privacy protection	<i>M</i>	4.65 _a	4.76 _{ab}	4.76 _{ab}	4.78 _{ab}	4.84 _b	4.88 _b
	<i>SD</i>	0.90	0.89	0.82	0.81	0.87	0.84

SD: standard deviation.
Using Holm’s sequential Bonferroni post hoc comparisons, within rows, means with no lower case subscript in common differ at $p < .05$.

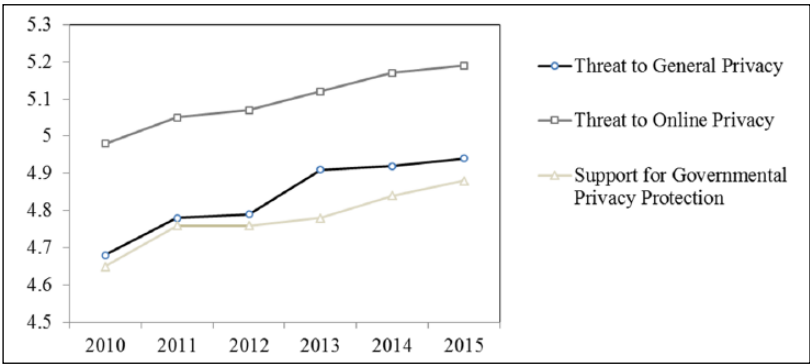


Figure 2. Trends in privacy perceptions between 2010 and 2015.

mediated the indirect paths between Facebook use and offline disclosure. Likewise, threat to general privacy ($\beta = -.20, p < .01$), threat to online privacy ($\beta = -.27, p < .001$), and support for governmental privacy protection ($\beta = -.16, p < .01$) mediated the indirect paths between Facebook use and online disclosure.

Trends in privacy perceptions

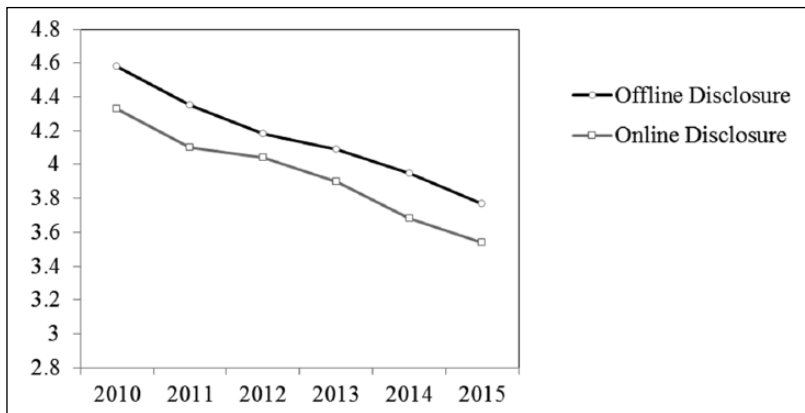
To address RQ1, a one-way analysis of variance showed statistically significant differences in privacy perceptions across the 5-year period (see Table 1 and Figure 2). Specifically, threat to general privacy, $F(5, 2783) = 5.13, p < .05$; threat to online privacy, $F(5, 2783) = 4.75, p < .05$; and support for governmental privacy protection, $F(5, 2783) = 3.22, p < .05$, gradually increased between 2010 and 2015. Post-hoc comparisons indicated that ratings for each privacy perception domain in 2015 were significantly higher than those in 2010.

Table 2. Trends in self-disclosure between 2010 and 2015.

Self-disclosure	Year						
		2010	2011	2012	2013	2014	2015
Offline self-disclosure	<i>M</i>	4.58 _a	4.35 _{ab}	4.18 _{bc}	4.09 _{cd}	3.95 _{de}	3.77 _e
	<i>SD</i>	0.71	0.74	0.69	0.79	0.83	0.80
Online self-disclosure	<i>M</i>	4.33 _a	4.10 _{ab}	4.04 _{bc}	3.90 _{cd}	3.68 _{de}	3.54 _e
	<i>SD</i>	0.68	0.76	0.74	0.82	0.78	0.75

SD: standard deviation.

Using Holm's sequential Bonferroni post hoc comparisons, within rows, means with no lower case subscript in common differ at $p < .05$.

**Figure 3.** Trends in self-disclosure between 2010 and 2015.

Trends in self-disclosure

To address RQ2, a one-way analysis of variance showed statistically significant differences from year to year in self-disclosure behaviors (see Table 2 and Figure 3). Specifically, offline self-disclosure, $F(5, 2778) = 12.89$, $p < .001$, and online self-disclosure, $F(5, 2783) = 44.02$, $p < .001$, steadily decreased between 2010 and 2015. Post-hoc comparisons showed that while there was no significant difference in self-disclosure between consecutive years, significant differences emerged, however, between 2-year intervals and beyond.

Changes in relationships between Facebook use and privacy perceptions

To address RQ3, a series of 2 (Facebook use: light, heavy) \times 6 (Year) analyses of variance were conducted on each of the three domains of privacy perceptions to determine if the relationships between Facebook use and privacy perceptions changed during the 5-year period. A median split was employed for each year to dichotomize Facebook use such that those reporting less than the median hours/day of Facebook use were categorized as

Table 3. Threat to general privacy: Facebook Use × Year interaction.

Facebook use	Year						
		2010	2011	2012	2013	2014	2015
Light	M	4.86 _{aB}	4.85 _{aB}	4.82 _{aA}	4.85 _{aA}	4.90 _{aA}	4.94 _{aA}
	SE	.06	.05	.05	.05	.05	.06
Heavy	M	4.39 _{aA}	4.55 _{bA}	4.69 _{cA}	4.84 _{dA}	5.01 _{eA}	5.04 _{eA}
	SE	.05	.05	.06	.05	.05	.06

SE: standard error.
Using Holm’s sequential Bonferroni post hoc comparisons, within rows, means with no lower case subscript in common differ at $p < .05$; within columns, means with no upper case subscript in common differ at $p < .05$.

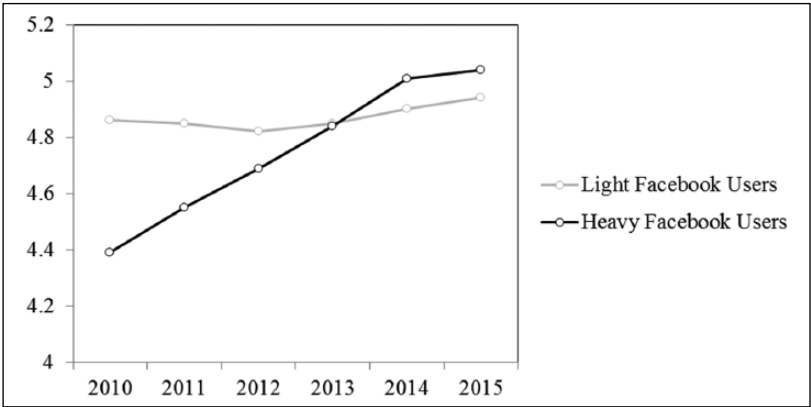


Figure 4. Threat to general privacy: Facebook Use × Year interaction.

light users and those reporting more than the median hours/day of Facebook use were categorized as heavy users. Although each of the analyses yielded significant main effects (i.e. heavier users indicated lower threat to general privacy, threat to online privacy, and support for governmental privacy protection, and these privacy concerns increased over the years), our primary interest was to examine the interaction effects.

Threat to general privacy. The analysis yielded a significant Facebook Use × Year interaction effect, $F(5, 2709) = 3.89, p < .01, \eta_p^2 = .01$ (see Table 3). Figure 4 illustrates that for light users, there was no significant year-to-year change in threat to general privacy. Yet, for heavy users, there was a significant positive linear trend for threat to general privacy. Moreover, in the earlier years of 2010 and 2011, the difference in threat to general privacy between light and heavy users was significant, whereas there was no significant difference from 2012 onward.

Threat to online privacy. The analysis revealed a significant Facebook Use × Year interaction effect, $F(5, 2709) = 5.75, p < .01, \eta_p^2 = .01$ (see Table 4). Figure 5

Table 4. Threat to online privacy: Facebook Use × Year interaction.

Facebook use	Year						
		2010	2011	2012	2013	2014	2015
Light	M	5.12 _{aB}	5.18 _{aB}	5.16 _{aB}	5.22 _{aA}	5.20 _{aA}	5.23 _{aA}
	SE	.05	.04	.04	.05	.05	.05
Heavy	M	4.42 _{aA}	4.67 _{bA}	4.84 _{cA}	5.10 _{dA}	5.14 _{dA}	5.17 _{dA}
	SE	.06	.06	.05	.05	.05	.05

SE: standard error.
Using Holm’s sequential Bonferroni post hoc comparisons, within rows, means with no lower case subscript in common differ at $p < .05$; within columns, means with no upper case subscript in common differ at $p < .05$.

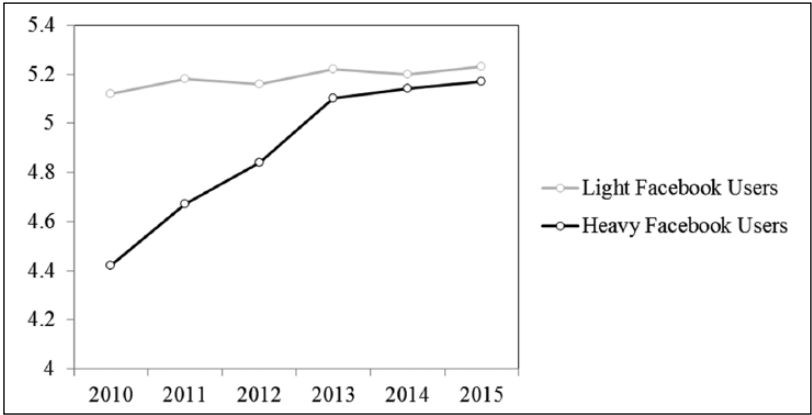


Figure 5. Threat to online privacy: Facebook Use × Year interaction.

illustrates that for light users, there was no year-to-year change in threat to online privacy. However, for heavy users, there was a significant positive linear trend for threat to online privacy, except between 2013 and 2015. Moreover, whereas in the earlier years between 2010 and 2012, the difference in threat to online privacy between light and heavy users was significant, there was no significant difference from 2013 onward.

Support for governmental privacy protection. The analysis yielded a significant Facebook Use × Year interaction effect, $F(5, 2709) = 5.92, p < .01, \eta^2_p = .01$ (see Table 5). Figure 6 illustrates that for light users, there was no year-to-year change in support for governmental privacy protection. Yet, for heavy users, there was a significant positive linear trend for support for governmental privacy protection from 2010 to 2011 and 2013 to 2015. Moreover, whereas in the earlier years of 2010 and 2011, the difference in support for governmental privacy protection between light and heavy users was significant, there was no significant difference from 2012 onward.

Table 5. Support for governmental privacy protection: Facebook Use × Year interaction.

Facebook use	Year						
		2010	2011	2012	2013	2014	2015
Light	M	4.83 _{aB}	4.78 _{aB}	4.72 _{aA}	4.79 _{aA}	4.81 _{aA}	4.86 _{aA}
	SE	.06	.05	.06	.06	.06	.05
Heavy	M	4.30 _{aA}	4.60 _{bA}	4.61 _{bA}	4.68 _{bA}	4.87 _{cA}	4.91 _{cA}
	SE	.05	.05	.06	.05	.05	.06

SE: standard error.
Using Holm’s sequential Bonferroni post hoc comparisons, within rows, means with no lower case subscript in common differ at $p < .05$; within columns, means with no upper case subscript in common differ at $p < .05$.

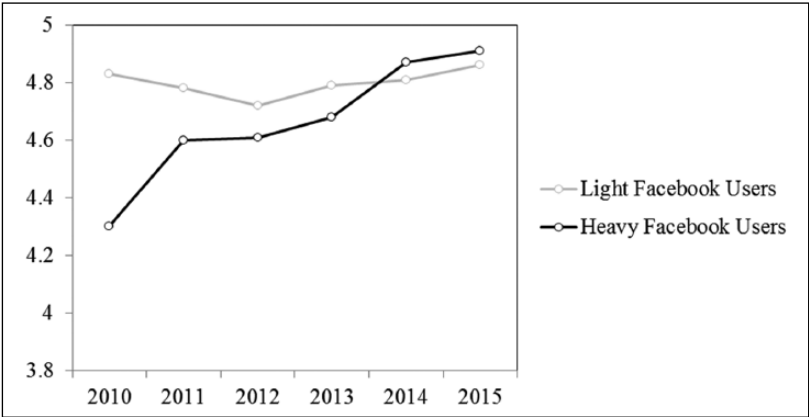


Figure 6. Support for governmental privacy protection: Facebook Use × Year interaction.

Changes in relationships between privacy perceptions and self-disclosure

To address RQ4, a series of multiple linear regressions were performed to determine whether the relationships between privacy perceptions and self-disclosure behaviors changed in the time frame between 2010 and 2015.

Offline self-disclosure. The analysis revealed a significant Threat to General Privacy × Year interaction ($\beta = .39, p < .01$) for offline disclosure. Specifically, threat to general privacy became a weaker negative predictor of offline disclosure as time progressed (2010: $\beta = -.32, p < .01$; 2011: $\beta = -.24, p < .01$; 2012: $\beta = -.19, p < .05$; 2013: $\beta = -.17, p < .05$; 2014: $\beta = -.14, p < .05$; 2015: $\beta = -.12, p < .05$). Similar patterns emerged for the other two privacy perception domains. A significant Threat to Online Privacy × Year interaction ($\beta = .27, p < .01$) for offline disclosure indicated that threat to online privacy became a weaker negative predictor of offline disclosure across the years (2010: $\beta = -.21, p < .01$; 2011: $\beta = -.18, p < .05$; 2012: $\beta = -.14, p < .05$; 2013: $\beta = -.10, p < .05$; 2014: $\beta = -.03, p < .05$; 2015: $\beta = -.02, p < .05$). Likewise, a significant Support for Governmental

Privacy Protection \times Year interaction ($\beta = .29, p < .01$) for offline disclosure revealed that support for governmental privacy protection became a weaker negative predictor of offline disclosure from year to year (2010: $\beta = -.19, p < .05$; 2011: $\beta = -.13, p < .05$; 2012: $\beta = -.13, p < .05$; 2013: $\beta = -.09, p < .05$; 2014: $\beta = -.02, p < .05$; 2015: $\beta = -.01, p < .05$).

Online self-disclosure. The analysis yielded a significant Threat to General Privacy \times Year interaction ($\beta = .31, p < .01$) for online disclosure. In particular, threat to general privacy became a weaker negative predictor of online disclosure with time (2010: $\beta = -.26, p < .01$; 2011: $\beta = -.23, p < .01$; 2012: $\beta = -.16, p < .05$; 2013: $\beta = -.14, p < .05$; 2014: $\beta = -.10, p < .05$; 2015: $\beta = -.07, p < .05$). Similar patterns emerged for the other two privacy perception domains. A significant Threat to Online Privacy \times Year interaction ($\beta = .37, p < .01$) for online disclosure indicated that threat to online privacy became a weaker negative predictor of online disclosure across the years (2010: $\beta = -.35, p < .01$; 2011: $\beta = -.32, p < .01$; 2012: $\beta = -.27, p < .01$; 2013: $\beta = -.20, p < .01$; 2014: $\beta = -.18, p < .05$; 2015: $\beta = -.14, p < .05$). Likewise, a significant Support for Governmental Privacy Protection \times Year interaction ($\beta = .21, p < .05$) for online disclosure revealed that support for governmental privacy protection became a weaker negative predictor of online disclosure from year to year (2010: $\beta = -.20, p < .01$; 2011: $\beta = -.18, p < .05$; 2012: $\beta = -.13, p < .05$; 2013: $\beta = -.08, p < .05$; 2014: $\beta = -.03, p < .05$; 2015: $\beta = -.02, p < .05$).

Discussion

Using cultivation theory as a framework to examine the pervasive theme of self-disclosure on SNSs, this research supports the expected overall relationship between Facebook use and more relaxed privacy attitudes, which subsequently led to greater self-disclosure in both online and offline contexts. These results suggest that SNSs serve a socializing role by conveying to users a reality where personal data are freely exchanged and self-disclosure is highly routinized. The influx of personal information in the virtual environment appears to cultivate perceptions of privacy such that users are less concerned about privacy risks and pay less attention to privacy safeguards. SNSs can thus be viewed as a collective symbolic environment where users learn about common themes and practices associated with high volumes of information disclosure. Applying a cultivation perspective to the context of social media, this study contributes to existing literature by confirming the socialization potential of SNSs to impact users' attitudes and beliefs pertaining to issues of privacy and self-expression.

However, when taking into consideration how these aforementioned relationships have changed during the previous 5 years, our longitudinal analysis yielded divergent patterns in the fluctuation of risk perceptions between light and heavy Facebook users. On the global level, although light Facebook users generally reported stronger risk perceptions, as compared to heavy Facebook users, the data revealed that their threats to general and online privacy and support for governmental privacy protection remained stable across time. This finding suggests that light consumption of social media has no influence over individuals' views on privacy. Yet, privacy concerns among heavy users steadily increased to comparable levels of light users. While the gap in risk perceptions between light and heavy users was more noticeable in the earlier years between 2010 and

2012, these differences subsided after 2012. In other words, the groups mainstreamed toward higher levels of privacy concerns.

Some explanations can be offered for these compelling trends. First, as heavy Facebook users are generally more exposed to personal data online, it is important to consider the functional use of this information. Whereas extensive research points to the prosocial effects of self-disclosure on impression formation and management and the strengthening of social bonds (Nosko et al., 2010), a number of antisocial effects are associated with the misuse of personal data. Specifically, frequent online activities of bullying, sexual and violent harassment, and clique formation have yielded a host of harmful psychological outcomes including anxiety, social isolation, privacy sensitivity, and depression (Hinduja and Patchin, 2010). Debatin et al. (2009) found that while Facebook was strongly perceived as a tool to enhance social connectedness, only when participants were asked to speak specifically about its role in stimulating gossip and rumors did they openly acknowledge partaking in such activities. Hence, it is possible that although social media offer meaningful opportunities to enrich social interactions, prolonged SNS consumption potentially exposes users to instances where privacy is abused. More extreme cases of privacy invasion may come in the form of hacking by computer experts. Such incidents have become much more common in recent years, increasing users' sensitivity to personal data (Federal Bureau of Investigation, 2015). Moreover, these breaches to security are extensively covered in the media which may further amplify awareness and fear of hacking, spam, spoof, and identity theft. This perhaps explains why threat to privacy and support for privacy safeguards escalated, particularly for heavy Facebook users across the years, whereas there was no change in these domains for those exhibiting light use.

Second, trends indicating the convergence in risk perceptions between light and heavy Facebook users may alternatively be informed by the process of technology diffusion. Specifically, individuals' abilities and motivations largely impact their likelihood to adopt innovations (Rogers, 2003). Early adopters tend to be those who are generally more motivated to adopt a technology, have greater self-efficacy, and appreciate the technology's symbolic value and meaning. It may be possible that heavy users of Facebook were the early adopters and are more motivationally driven, more confident about their skills in using the platform, and perceive the SNS as more positively gratifying than light users, implicit in their high consumption patterns. Given these user characteristics, it is understandable why in the initial years of our study, those who were more heavily engaged with Facebook reported significantly lower levels of privacy concerns. However, our study is limited in that data concerning the number of years users have been active on the site were not captured. Thus, future research should certainly consider examining SNS adoption patterns in order to better explain and predict privacy attitude trends. Furthermore, as knowledge acquisition is a central component of the diffusion process (Rogers, 2003), when users engage with a technology, they naturally learn about its affordances, benefits, and risks with time. Heavier users are more likely to attain such knowledge in greater quantities and at a faster rate due to the intensity and duration of their involvement. Hence, this increased familiarity with and sensitivity to the Facebook environment and potential exposure to personal privacy risks may have contributed to the gradual increase in their threat to privacy. On the contrary, knowledge acquisition

occurs at a slower rate for light users, thus explaining why light consumption produced no noticeable changes in attitudes toward privacy.

At the global level, this study also found that individuals with more relaxed privacy attitudes had a greater tendency to self-disclose in both offline and online environments, corroborating the attitude–behavior link proposed by TRA (Fishbein and Ajzen, 1975) and the notion that personal information disclosure is highly regulated by privacy control mechanisms (Derlega and Chaikin, 1977; Petronio, 2002). However, our trend data show striking patterns such that the negative relationships between privacy perceptions and self-disclosure practices weakened as time progressed. In other words, users' threats to general and online privacy and support for governmental privacy protection became less robust predictors of personal information exchange across the 5-year period. These findings are potentially explained by the notion that light and heavy Facebook users mainstreamed toward higher levels of perceived privacy threat. Furthermore, there are perhaps factors outside of privacy risk perceptions that account for variations in self-disclosure. For example, as relationships develop, trust becomes even more important in building self-confidence and ensuring relational certainty (Mietzner and Lin, 2005). Therefore, it is possible that over time, the role of trust carries even more weight in predicting self-disclosure practices than the risks associated with the environment in which personal information exchange occurs.

The present research further supports the important mediating role of privacy attitudes, specifically threat to privacy and support for privacy safeguards, in the indirect effects of Facebook use on self-disclosure. This finding is consistent with previous studies showing that the consumption of SNSs does not directly drive disclosure behaviors (Acquisti and Gross, 2006; Stutzman et al., 2011), but rather other intervening variables related to risk perceptions need to be considered. Therefore, in order for SNSs to maintain a climate inundated with rich information exchange, they need to ensure that perceptions of safety, transparency, and security are relatively high, placing users in an environment of minimal risk. Alternatively, researchers also suggest that users deploy privacy controls during their self-disclosures. Social stenography entails the use of intricate strategies such as smuggling meaning via in-group references to achieve privacy goals (boyd and Marwick, 2011). Hogan's (2010) lowest common denominator approach argues that individuals limit their content to the extent that it will be appropriate for all members of the network. Other scholars have found that people deliberately use multiple networks, platforms, and profiles to manage their privacy (Vitak et al., 2015). Such variation in information exchange behaviors demonstrates that not all disclosures are treated equally and that privacy is inherently valued.

Interestingly, the findings from this study also show similar patterns in the way privacy attitudes pertaining to both global and virtual domains predict offline and online disclosures. These results point to similarities in the nature of FTF and CMC interpersonal exchanges (Lampe et al., 2007), suggesting that these spaces are potentially interchangeable. Likewise, our research supports the work of Baym (1996), boyd (2007), and Marwick (2013) which discounts the idea that individuals have separate online and offline identities evident in the ways in which SNSs have become highly integrated and routinized in our everyday practices (Debatin et al., 2009). These results bolster the notion that disclosure patterns are no different in CMC conditions than they are in FTF

interactions, disconfirming the media richness perspective that greater self-disclosure is required to compensate for the lack of non-verbal and social cues online (Walther, 1996).

Additional trends are worth noting, particularly the progressive decline in Facebook use and offline and online disclosure and the steady increase in threat to general privacy, threat to online privacy, and support for governmental privacy protection during the past 5 years. Although Facebook remains the most popular SNS among adults, its overall growth has slowed down (Pew Research Center, 2015). Recent survey data show that users of SNSs such as Instagram, LinkedIn, Pinterest, and Twitter have increased at a faster rate than those of Facebook between 2012 and 2014. Moreover, multi-platform use has become more common such that 52% of adults online now use at least two SNSs. These findings from the Pew Research Center (2015) help explain the decrease in the number of hours people are spending on Facebook as was found in our study. Additionally, the contrasting patterns between Facebook use and risk perceptions in our data to some extent can be informed by the uses and gratifications approach. In the context of our research, privacy concerns could impact the anticipated gratifications sought from Facebook. Therefore, the decline in Facebook usage potentially reflects the lower perceived benefits or higher risks associated with its consumption. For example, the increase in criminal acts (e.g. identity theft, fraud, and computer hacking) in recent years, most notably the Edward Snowden leaks, may have contributed to the escalation of online privacy and security concerns among those in our sample. Moreover, during the 5-year period of our study, Facebook made various platform changes that received public scrutiny about privacy which could have impacted users' attitudes and disclosure of personal information. However, these trends should be interpreted with caution as the directionality of these variables is unclear. While it is possible that increased threat to privacy reduced Facebook use which inevitably fostered less self-disclosure due to users' absence on the platform, alternatively, some individuals may innately have more relaxed privacy boundaries. This relative ease and desire for disclosure could be linked to relatively low risk perceptions, propelling them to naturally gravitate toward SNSs that offer opportunities to satisfy their disclosure needs. Our trend analysis is limited in not allowing us to make causal claims among the variables of interest in this study. Therefore, future research should certainly consider employing a panel longitudinal design that follows the same people over time or experimental methods to precisely establish causality among SNS usage, privacy perceptions, and self-disclosure practices.

Another limitation of our study is that we sampled from a college population and the gender and racial composition of the sample is not evenly distributed, raising an external validity issue. Research has shown that younger users not only are less aware of privacy invasion risks, but also generously disclose personal information in their profiles (Taraszow et al., 2010). However, as students mature, particularly as they seek job opportunities, there may be growing concerns about future bosses seeing old photos from their college years (Sherman, 2013), consequently explaining a change in privacy attitudes and behaviors among the heavy users of Facebook in our study. Alternatively, it is also possible that the longer users are on Facebook, the more their audience diversifies, thus making users more aware of their privacy concerns (Binder et al., 2009; Vitak, 2012). Therefore, future research should consider contextual factors and the duration of time that users are active on SNSs. Furthermore, our study relied on self-reported measures of

personal information exchange rather than actual content shared by SNS users. Future researchers may consider coding the nature of actual information exchange as individuals perhaps have different interpretations of what constitutes as personal or private data. Additionally, factors aside from threat to privacy and support for privacy safeguards may mediate the paths between SNS usage and self-disclosure such as interpersonal trust (Kim et al., 2006) and the valence of self-disclosure outcomes (Utz, 2015). The consideration of these variables in future research will help us gain a more comprehensive understanding of SNSs' effects on disclosure practices.

Conclusion

The current investigation into the impact of SNS use on attitudes and behaviors associated with privacy and self-expression has important theoretical implications. First, this research uniquely applies a cultivation perspective (Morgan et al., 2015) to support the way SNSs potentially affect users' conceptions of reality. The omnipresence of self-disclosure in the virtual world represents a reality where the revelation of personal data may not only be perceived as exceedingly habitual, but also expected. Therefore, this study emphasizes the socializing and cultivating capacity of SNSs, particularly in the way prolonged use may have cumulative effects on people's privacy boundaries and the disclosure that is regulated by these boundaries. Second, the longitudinal nature of this research allows us to forecast patterns in the effects of SNS use on privacy perceptions and the exchange of personal information. The recent convergence in risk perceptions among light and heavy users points to the mitigating effect of SNS use on estimated threats to privacy. A ceiling effect could be occurring with perceived risk. This could also explain the diminishing negative relationships between privacy concerns and self-disclosure, alternatively suggesting potential desensitization effects.

This study invaluablely contributes to the existing body of literature on issues of privacy and self-disclosure on SNSs. This longitudinal analysis offers a more comprehensive and meaningful perspective of the trends in privacy perceptions and disclosure behaviors among SNS users during the past 5 years. As the diversification and the accessibility of SNSs continue to grow, examining changes in information dissemination and privacy boundary regulations become increasingly important to further understand how personal identities are created, developed, and managed over time.

Funding

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

References

- Acquisti A and Gross R (2006) Imagined communities: awareness, information sharing and privacy on Facebook. In: *6th workshop on privacy enhancing technologies*, Cambridge, 28–30 June.
- Altman I (1975) *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole Publishing.

- Baym NK (1996) The emergence of community in computer-mediated communication. In: Shields R (ed.) *Cultures of Internet: Virtual Spaces, Real Histories, Living Bodies*. London: SAGE, pp. 138–163.
- Binder H, Howes A and Sutcliffe A (2009) The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Boston, MA, 7 April, pp. 965–974. New York: ACM.
- boyd d (2007) Why youth (heart) social network sites: the role of networked publics in teenage social life. In: Buckingham D (ed.) *MacArthur Foundation Series on Digital Learning Youth, Identity, and Digital Media Volume*. Cambridge, MA: The MIT Press, pp. 119–142.
- boyd d and Ellison NB (2007) Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13(1): 210–230.
- boyd d and Marwick A (2011) Social steganography: privacy in networked publics. In: *Paper presented at the international communication association conference*, Boston, MA, 28 May.
- Davis K and James C (2012) Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology* 38(1): 4–25.
- Debatin B, Lovejoy JP and Horn AK (2009) Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15(1): 83–108.
- Derlega VJ and Berg JH (eds) (1987) *Self-Disclosure: Theory, Research, and Therapy*. New York: Plenum Press.
- Derlega VJ and Chaikin A (1977) Privacy and self-disclosure in social relationships. *Journal of Social Issues* 33(3): 102–115.
- Dudo A, Brossard D, Shanahan J, et al. (2011) Science on television in the 21st century: recent trends in portrayals and their contributions to public attitudes toward science. *Communication Research* 38(6): 754–777.
- Dwyer C, Hiltz SR and Passerini K (2007) Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. In: *Proceedings of the thirteenth Americas conference on information systems*, Keystone, CO, 31 December.
- Facebook (2016) Newsroom (statistics). Available at: <http://newsroom.fb.com/company-info/>
- Federal Bureau of Investigation (2015) Internet crime reports. Available at: <http://www.ic3.gov/media/annualreports.aspx>
- Fishbein M and Ajzen I (1975) *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.
- Fogel J and Nehmad E (2009) Internet social network communities: risk taking, trust, and privacy concerns. *Computers in Human Behavior* 25: 153–160.
- Gerbner G (1969) Toward cultural indicators: analysis of mass mediated public message systems. *AV Communication Review* 17: 137–148.
- Gerbner G, Gross L, Morgan M, et al. (1994) Growing up with television: the cultivation perspective. In: Bryant J and Zillmann D (eds) *Media Effects: Advances in Theory and Research*. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., pp. 17–41.
- Gibbs JL, Ellison NB and Lai CH (2011) First comes love, then comes Google: an investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research* 38(1): 70–100.
- High AC and Caplan SE (2009) Social anxiety and computer-mediated communication during initial interactions: implications for the hyperpersonal perspective. *Computers in Human Behavior* 25(2): 475–482.
- Hinduja S and Patchin JW (2010) Bullying, cyberbullying, and suicide. *Archives of Suicide Research* 14(3): 206–221.

- Hogan B (2010) The presentation of self in the age of social media: distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society* 30(6): 377–386.
- Kim PH, Dirks KT, Cooper CD, et al. (2006) When more blame is better than less: the implications of internal vs. external attributions for the repair of trust after a competence- vs. integrity-based trust violation. *Organizational Behavior and Human Decision Processes* 99: 49–65.
- Lampe C, Ellison N and Steinfield C (2007) A Face(book) in the crowd: Social searching vs. social browsing. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Banff, AB, Canada, 4–8 November, pp. 434–444. New York: ACM Press.
- Lyon D and Zureik E (1996) Surveillance, privacy, and the new technology. In: Lyon D and Zureik E (eds) *Computers, Surveillance, and Privacy*. Minneapolis, MN: University of Minnesota Press, pp. 1–18.
- Marwick A (2013) Online identity. In: Harley J, Burgess J and Bruns A (eds) *Companion to New Media Dynamics* (Blackwell Companions to Cultural Studies). Malden, MA: Blackwell, pp. 355–364.
- Mietzner S and Lin LW (2005) Would you do it again? Relationship skills gained in a long-distance relationship. *College Student Journal* 39(1): 192–200.
- Morgan M, Shanahan J and Signorielli N (2015) Yesterday's new cultivation, tomorrow. *Mass Communication & Society* 18(5): 674–699.
- Nguyen M, Bin YS and Campbell A (2012) Comparing online and offline self-disclosure: a systematic review. *Cyberpsychology, Behavior and Social Networking* 15(2): 103–111.
- Nosko A, Wood E and Molema S (2010) All about me: disclosure in online social networking profiles: the case of Facebook. *Computers in Human Behavior* 26(3): 406–418.
- Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press.
- Pew Research Center (2014) Social networking fact sheet. Available at: <http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/> (accessed 1 August 2015).
- Pew Research Center (2015) Social media update 2014. Available at: <http://www.pewinternet.org/2015/01/09/social-media-update-2014/> (accessed 1 September 2015).
- Rogers EM (2003) *Diffusion of Innovations*. 5th ed. New York: Free Press.
- Shanahan J and Morgan M (1999) *Television and Its Viewers: Cultivation Theory and Research*. Cambridge: Cambridge University Press.
- Sherman E (2013) 1 in 10 young job hunters rejected because of their social media. Available at: <http://jobs.aol.com/articles/2013/06/0/applicants-rejected-social-media-on-device-research/> (accessed 20 May 2015).
- Shrum LJ, Wyer RS and O'Guinn TC (1998) The effects of television consumption on social perceptions: the use of priming procedures to investigate psychological processes. *Journal of Consumer Research* 24: 447–458.
- Signorielli N and Lears M (1992) Children, television, and conceptions about chores: attitudes and behaviors. *Sex Roles* 27: 157–170.
- Smith HJ, Milberg SJ and Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* 20: 167–196.
- Spencer SB (2002) Reasonable expectations and the erosion of privacy. *San Diego Law Review* 39: 843–911.
- Stone E, Geutal HG, Gardner DG, et al. (1983) A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology* 68: 459–468.
- Stutzman F, Capra R and Thompson J (2011) Factors mediating disclosure in social network sites. *Computers in Human Behavior* 27: 590–598.

- Subrahmanyam K, Reich SM, Waechter N, et al. (2008) Online and offline social networks: use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology* 29: 420–423.
- Taraszow T, Aristodemou E, Shitta G, et al. (2010) Disclosure of personal and contact information by young people in SNSs: an analysis using Facebook profiles as an example. *International Journal of Media and Cultural Politics* 6(1): 81–98.
- Tavani HT and Grodzinsky FS (2002) Cyberstalking, personal privacy, and moral responsibility. *Ethics and Information Technology* 4: 123–132.
- Utz S (2015) The function of self-disclosure on social networking sites: not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. *Computers in Human Behavior* 45: 1–10.
- 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.
- Vitak J, Blasiola S, Patil S, et al. (2015) Balancing audience and privacy tensions on social network sites. *International Journal of Communication Systems* 9: 1485–1504.
- Walther JB (1996) Computer-mediated communication: impersonal, interpersonal and hyperpersonal interaction. *Communication Research* 23(1): 3–43.

Author biographies

Mina Tsay-Vogel is an assistant professor in the Department of Mass Communication, Advertising & Public Relations and Co-Director of the Communication Research Center at Boston University. Her research interests include media effects, entertainment psychology, and social media use and influence.

James Shanahan is dean of the Media School at Indiana University. His research interests include cultural indicators, cultivation theory, media effects, and environmental communication.

Nancy Signorielli is a professor in the Department of Communication at the University of Delaware. Her research interests include content studies, cultivation analysis, media effects, and media and children.