The Journal of Social Psychology, 154: 352–369, 2014

ISSN: 0022-4545 print / 1940-1183 online
DOI: 10.1080/00224545.2014.914881

Routledge
Taylor & Francis Group

Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior

ALEXANDER K. SAERI
CLAUDETTE OGILVIE
STEPHEN T. LA MACCHIA
University of Queensland

JOANNE R. SMITH
University of Exeter

WINNIFRED R. LOUIS
University of Queensland

ABSTRACT. The present research adopts an extended theory of the planned behavior model that included descriptive norms, risk, and trust to investigate online privacy protection in Facebook users. Facebook users ($N = 119$) completed a questionnaire assessing their attitude, subjective injunctive norm, subjective descriptive norm, perceived behavioral control, implicit perceived risk, trust of other Facebook users, and intentions toward protecting their privacy online. Behavior was measured indirectly 2 weeks after the study. The data show partial support for the theory of planned behavior and strong support for the independence of subjective injunctive and descriptive norms. Risk also uniquely predicted intentions over and above the theory of planned behavior, but there were no unique effects of trust on intentions, nor of risk or trust on behavior. Implications are discussed.

Keywords: Facebook, online privacy, theory of planned behavior

THE EXPLOSIVE GROWTH OF THE INTERNET has changed the way people live their lives. By mid-2012, 2.4 billion people were connected worldwide (Internet World Stats, 2014). The Internet, now accessible from pocket-sized devices and integrated with our daily lives, can no longer be considered separate from the "real world" (Boyd & Ellison, 2007; Schofield & Joinson, 2008). The concept of informational privacy thus becomes a clear concern for Internet users: Information disclosed on the Internet can be kept forever without degradation, can be accessed or copied without the discloser knowing, and can easily be searched and integrated from disparate sources (Sparck-Jones, 2003).

Address correspondence to Winnifred R. Louis, University of Queensland, Department of Psychology, McElwain Bldg., UQ, St. Lucia, 4072 Queensland, Australia. E-mail: w.louis@psy.uq.edu.au

Breaches of online privacy can have great social, financial, and psychological costs (Schofield & Joinson, 2008; Whitty & Joinson, 2008). Embarrassing photographs or "private" conversations may be disseminated to any number of individuals (Whitty & Joinson, 2008), or personally identifiable information may be stolen for identity fraud (Electronic Frontiers Australia, 2006). It is psychologically threatening to experience the loss of control associated with a breach of privacy (Margulis, 2003).

Research into online privacy and its antecedents are critical in a world where the integration of online and offline identities and the consequences of privacy breaches can only grow (Whitty & Joinson, 2008). The present research contributes to this emerging research focus by examining online privacy protection in Facebook users in relation to the theory of planned behavior (Ajzen, 1991), while also considering the role of descriptive norms, perceived risk, and trust.

Facebook is a popular website (http://www.facebook.com) where individuals can post photos, personal information, and news about themselves in a shared space that can be made accessible to other users in varying degrees. For example, information may be set to be visible to the public or shared with "friends" (several thousand may be nominated), as well as "friends of friends" and other variations. Understanding the antecedents of online privacy protection is critical, as many individuals fail to protect their Facebook privacy online securely (Christofides, Muise, & Desmarais, 2012). Importantly, disclosure on platforms such as Facebook can elicit positive social support, not just bullying or victimization (McCabe & Ricciardelli, 2003). More broadly, the explosive growth in the numbers of individuals who use social networking sites such as Facebook, and its increasing centrality within their social lives, has fuelled a corresponding wave of social science research (e.g., Greitemeyer & Kunz, 2013; Milyavskaya, Reoch, Koestner, & Losier, 2010). The current study extends previous work on privacy concerns by examining online privacy protection in the context of social network services and social media, an emerging nexus of research and applied concern.

The Theory of Planned Behavior

The theory of planned behavior (TPB; Ajzen, 1991) directly predicts individuals' behavior from relevant intentions and uniquely predicts these intentions from relevant attitudes, subjective norms, and perceived behavioral control. TPB has demonstrated efficacy as a conceptual framework for examining the antecedents of behaviors and effecting behavior change. It has been used to examine consumer behaviors (Smith, Terry, Manstead, Louis, Kotterman, & Wolfs, 2008), health behaviors (Duncan, Forbes-McKay, & Henderson, 2012; Karimi-Shahanjarini et al., 2012; Louis, Davies, Smith, & Terry, 2007), social-responsibility behaviors such as energy conservation (Nolan, Schultz, Cialdini, Goldstein, & Griskevicus, 2008) and charitable intentions to donate (Knowles, Hyde & White, 2012), and hundreds of other behaviors (see Armitage & Conner, 2001; Chudry, Foxall, & Pallister, 2011; Manning, 2009; McLachlan & Haggar, 2011).

In recent years, researchers have examined the utility of the TPB in relation to online behaviors, such as Facebook use among college students (Cameron, Ginsburg, Westhoff, & Mendez, 2012), partner-monitoring behavior on Facebook (Darvell, Walsch & White, 2011), online stock trading (Lee, 2009), and online privacy protection (Yao & Linz, 2008; Yousafzai, Foxall, & Pallister, 2010). In the domain of online privacy protection, attitudes and intentions have generally been significant predictors of behavior, with less support for the role of norms (Yousafzai

et al., 2010). However, affective variables have also been found to predict privacy protection, such as fear of crime (Yao & Linz, 2008) and trust (Yousafzai et al., 2010). The current research extends the theory of planned behavior by examining for the first time the independent roles of injunctive and descriptive norms in the context of online privacy protection.

Injunctive and Descriptive Norms

Although the theory of planned behavior is a robust and efficacious framework for investigating antecedents of behavior, the subjective norm component is commonly the weakest predictor of behavior (e.g., Ajzen, 1991; Armitage & Conner, 2001; Yao & Linz, 2008). Yet, as Cialdini and colleagues (1990, 1991) have argued, injunctive norms (what others approve or disapprove of) and descriptive norms (what others actually do) are distinct norm components that may be independent predictors of behavior (Cialdini, Reno, & Kallgren, 1990; Cialdini, Kallgren, & Reno, 1991; Cialdini et al., 2006; Louis et al., 2007). Thus, social influence will be underestimated if researchers fail to conceptualize injunctive norms and descriptive norms as separate constructs, and empirical research confirms this to be the case (Manning, 2009), particularly when the norms are incongruent (Smith & Louis, 2008). As a result, it is now generally recommended that TPB studies distinguish between injunctive and descriptive norms (Ajzen, 2006).

The distinction between injunctive and descriptive norms might also be particularly important in the context of online privacy protection. This is because anecdotal evidence suggests that online privacy may be an example of misaligned norms: socially significant others may almost unanimously approve of privacy protection but fail to enact it themselves. If this is the case, then it becomes critical to understand the relative predictive power of each type of norm in this context. Thus the present research examines independently the effects of injunctive and descriptive norms on online privacy protection behavior.

Risk and Trust: Affective Routes to Online Privacy Protection

The theory of planned behavior can be considered a rational-cognitive model of decision-making, in that individuals are assumed to weigh up attitudes, norms, and control in forming intentions and actions. However, this assumption has been criticized by some researchers, who have called for the inclusion of affective variables within the model (e.g., Ajzen & Driver, 1992; French et al., 2005; Lowe, Eves, & Carroll, 2002). Two important affective variables that are likely to be particularly relevant in relation to online privacy protection are perceived risk and perceived trust (see Lee, 2009; Paine, Reips, Steiger, Joinson, & Buchanan, 2007). The present study takes an integrative approach in predicting online privacy protection by investigating established TPB variables simultaneously with the affective variables of perceived risk and perceived trust.

The role of risk. Risk perceptions are important cues in social judgments (Jørgensen, Bäckström, & Björklund, 2013), serving as a warning of potential negative consequences of pursuing some action (Youn & Hall, 2008). Risk perceptions predict intentions in health and academic domains, over and above the TPB (Schmiege, Bryan, & Klein, 2009). In the context of online privacy, examination of perceived risk is particularly important due to how individuals

interact with the Internet. Despite the potential risks of information disclosure without consent or control online, the illusion of personal contact on the Internet (particularly in social network websites) may in fact reduce perceptions of risk (Youn & Hall, 2008).

Perceiving online activities as risky is associated with reduced service use (Lee, 2009) and with increased privacy protection (Alter & Oppenheimer, 2009; Paine et al., 2007; Youn & Hall, 2008). However, past work on risk and privacy protection may have confounded perceived risk with positive attitudes toward privacy protection by conceptualizing risk as "privacy concerns" (Paine et al., 2007). The present study extends previous work by simultaneously examining TPB and implicit perceived risk in predicting online privacy protection behavior.

The role of trust. Trust underpins any positive relationship; it is the willingness of one party to act or speak in such a manner that they are made more vulnerable to the other party (Cozby, 1973). One way to create trust is through self-disclosure (Rotter, 1980): by disclosing personal or private information, rapport and intimacy in interpersonal relationships is increased, and individuals are perceived as more trustworthy themselves (Henderson & Gilding, 2004). Trust can signal and elicit social support, which has important positive outcomes, including in online contexts (Ling, Chuang, & Hsaio, 2012). However, trust also extends beyond interpersonal relationships: trust in a commercial organization encourages disclosure of personal information (Metzger, 2004; Whitty & Joinson, 2008). Recent research into online privacy has found a negative association between trust and privacy protection (Christofides et al., 2012; for a review, see Wang & Emurian, 2005).

An important conceptual issue regarding trust and online privacy protection is the question of whom an individual is trusting or mistrusting online. Trust can occur at both the interpersonal and group level, with individuals trusting members of their own group more than members of other groups (Foddy, Platow, & Yamagishi, 2009), a concept known as depersonalized ingroup trust. By default, personal information disclosed on a Facebook profile is available to the individual's friends group (i.e., other users of the site with whom an individual has affirmed an individual connection). However, the individual cannot know who of their Friends are accessing their personal information, thus exhibiting depersonalized ingroup trust. If that individual chooses to allow their information to be seen by a wider audience, such as all Facebook users or all friends of their friends, group-level trust becomes even more relevant. The present study extends previous work by investigating the association between depersonalized ingroup trust and online privacy protection on Facebook.

The Present Study

The present study aims to make three specific contributions to theory. First, the present research extends the theory of planned behavior literature by investigating the novel online behavior of online privacy protection in an explicitly social context. Second, the current study integrates theory of planned behavior with norm focus theory by examining both subjective injunctive norms and subjective descriptive norms in predicting online privacy protection. In doing so, the study contributes to a more nuanced and comprehensive understanding of how normative influence can shape behavior. Finally, the research seeks to bridge the rational-cognitive theory of planned behavior with the more affective variables of perceived risk and perceived trust in online privacy protection. By simultaneously examining the attitudes, subjective norms, perceived

behavioral control, risk, and trust, the present research takes the first steps toward a more complete understanding of the processes that lead individuals to (or fail to) protect their privacy online.

A longitudinal observational study was conducted to fulfill these aims. Theory of planned behavior measures—including independent measurement of injunctive and descriptive norms—were recorded, as were perceived risk and perceived trust; an implicit measure of perceived risk was used in order to reduce confounds associated with "privacy concerns" scales (Youn, 2009; Youn & Hall, 2008). Importantly, an objective measure of online privacy protection behavior was recorded 2 weeks following the study based on the information publicly available on participants' Facebook profiles.

Hypotheses were specified in line with previous research examining TPB and online behavior (d'Astous et al., 2005; Darvell, Walsh, & White, 2011; Yousafzai et al., 2010). More positive attitudes toward online privacy protection would be associated with increased intentions to protect privacy online. Participants who perceived that important others approved of online privacy protection (subjective injunctive norm) would report increased intentions to protect their online privacy. Participants who perceived that important others were likely to protect their own privacy (subjective injunctive norm) would report increased intentions to protect their online privacy. Participants who perceived that they could control whether their privacy was protected online (perceived behavioral control) would report increased intentions to protect their online privacy. In line with previous research examining perceived risk (Lee, 2009) and trust (Wang & Emurian, 2005), it was expected that greater perceived risk and lower trust would independently be associated with increased intentions to protect privacy. In addition, it was predicted that perceived risk and trust would predict privacy protection intentions over and above the theory of planed behavior variables of attitudes, subjective injunctive and descriptive norms, and perceived behavioral control. Finally, it was predicted that intentions to predict privacy online would be associated with increased online privacy protection behavior two weeks later.

METHOD

Participants

A convenience sample of 119 first-year psychology students from an Australian university, who were also Facebook users, participated in return for partial course credit. Participants who suspected the study's true purpose ($n = 7$) or who did not follow researcher instructions ($n = 1$) were excluded from analysis. The final sample ($N = 111$) included 43 men and 68 women. Participants' ages ranged from 17 to 40 years ($M = 18.45$, $SD = 3.19$).

Design

Participants' intentions to protect their privacy on Facebook and actual privacy protection behavior measured two weeks following the study (T2 behavior) served as dependent measures. The theory of planned behavior variables (attitudes, subjective injunctive norm, subjective descriptive norm, and perceived behavioral control) were also measured, as were age and gender. Trust of other Facebook users and perceived risk were included as potential independent predictors of privacy protection intentions and behavior.

Procedure

The study was conducted in an Internet-connected laboratory in groups of up to 10. Participants first read an information sheet about online privacy protection and then completed a booklet with measures of perceived risk and trust, the theory of planned behavior variables (intentions, attitudes, injunctive and subjective descriptive norms, and perceived behavioral control), and age and gender. Two free-response items were used to probe for suspicion of study hypotheses.

When each participant completed their questionnaire, the researcher collected the questionnaire and handed the participant a separate sheet requesting that participants disclose their Facebook profile name for a researcher to access their public Facebook after 2 weeks. Most ($N = 107$, 96%) participants chose to provide consent. After all participants had chosen whether or not to provide consent, participants were debriefed both verbally and in writing.

Measures

Perceived risk. A word-stem completion task adapted from previous research (Alter & Oppenheimer, 2009) was used to assess perceived risk implicitly. Participants were asked to think of the context in which they most often accessed Facebook before completing a task in which they provided a missing letter for each of 15 word-stems. Eight of the word-stems could be completed to form risk-related words (e.g., "sc_re" could be completed as "score" or scare"; "concer_" could be completed as "concern" or "concert"). The other seven word-stems were fillers; they could be completed to form neutral words (e.g., "_ook" could be completed as "book", or "look"). Perceived risk was calculated as the proportion of risk-related word stems completed as risk-related words, with higher scores indicating greater perceived risk.

Trust. Two items adapted from an previously validated scales of trust (Dunn & Schweitzer, 2005; Kenworthy & Jones, 2009) were used to measure trust of Facebook users as a group ("I trust all Facebook users" and "I think all Facebook users are likely to be trustworthy"; measured on a 7-point scale ranging from 1 [*strongly agree*] to 7 [*strongly disagree*]). Items were averaged to form a reliable scale with higher scores indicating greater trust ($r = .49$, $p < .001$).

Attitudes. Participants' attitudes toward protecting their privacy online were assessed using five semantic differential items adapted from previous TPB research (Ajzen, 2006; Smith & Louis, 2008). Items were rated on a 7-point scale; three items were positively scored (e.g., "When I personally think about protecting my privacy on Facebook by controlling access to my personal information over the next two (2) weeks, I consider doing so to be"; measured on a 7-point scale ranging from 1 [*worthless*] to 7 [*valuable*]). Two items were reverse-scored (e.g., from 1 [*pleasant*] to 7 [*unpleasant*]). Items were averaged to form a reliable scale with higher scores indicating more positive attitudes toward online privacy protection ($\alpha = .82$).

Subjective injunctive norm. Interpersonal subjective injunctive norms toward online privacy protection were assessed with a four-item measure adapted from previous TPB research (Ajzen, 2006; Cialdini et al., 1991). The items were rated on a 7-point scale; two were positively scored (e.g., "Most people important to me think that for me to protect my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two

[2] weeks is"; ranging from 1 [*bad*] to 7 [*good*]). Two items were reverse-scored (e.g., "People who are important to me think that I ____ protect my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*should*] to 7 [*should not*]). Scores on the items were averaged to form a reliable scale, with higher scores indicating a more positive subjective injunctive norm ($\alpha = .65$).

Subjective descriptive norm. Interpersonal subjective descriptive norms toward online privacy protection were assessed with a four-item measure derived from previous TPB research (Ajzen, 2006; Cialdini et al., 1991). Items were rated on a 7-point scale. Two items were positively scored (e.g., "People who are important to me would protect their privacy on Facebook by controlling access to their personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*very unlikely*] to 7 [*very likely*]). Two items were reverse-scored (e.g., "The people in life whose opinions I value would _____ their privacy on Facebook by controlling access to their personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*protect*] to 7 [*not protect*]). Scores on the items were averaged to form a reliable scale, with higher scores indicating a more positive subjective descriptive norm ($\alpha = .69$).

Perceived behavioral control. Perceptions of control over online privacy protection behavior were assessed using a four-item measure adapted from previous TPB research (Ajzen, 2006; Smith et al., 2012). Items were rated on a 7-point scale; one item was positively scored (i.e., "I think I have ____ over protecting my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*no control at all*] to 7 [*complete control*]). Three items were reverse-scored (e.g., "For me to protect my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two [2] weeks is"; ranging from 1 [*very easy*] to 7 [*very difficult*]). Items were averaged to form a reliable scale, with high scores indicating greater perceived behavioral control ($\alpha = .63$).

Intentions. A four-item measure adapted from previous research (Ajzen, 2006; Smith et al., 2012) was used to assess participants' intentions to protect their privacy online. Items were rated on a 7-point scale; one item was positively scored (i.e., "I intend to protect my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*very unlikely*] to 7 [*very likely*]). Three items were reverse-scored (e.g., "I expect to protect my privacy on Facebook by controlling access to my personal information using the privacy settings over the next two [2] weeks"; ranging from 1 [*completely true*] to 7 [*completely false*]). Items were averaged to form a reliable scale, with higher scores indicating greater intentions to engage in online privacy protection ($\alpha = .91$).

Behavior. A researcher searched for consenting participants' profiles on Facebook using information provided. The researcher recorded whether a participant disclosed each of 22 types of personal information (e.g., profile photo, interests, birthday, current location). The behavior measure was recorded 14 days following the first session. The total number of items of disclosed information (out of 22) was reverse-coded so that higher scores indicated greater privacy protection behavior.

RESULTS

Descriptive Statistics

The means, standard deviations and bivariate correlations for all variables are presented in Table 1. Overall, participants reported positive attitudes, high perceived behavioral control, and high intentions to protect their privacy on Facebook. Although the subjective injunctive norm was significantly more supportive of privacy protection than the subjective descriptive norm ($t[110] = 7.88$, $p < .001$), both were above the midpoint of the scale and thus significantly positive ($ps < .001$). Participants completed about half of the risk-related word stems with risk-related words, and generally reported low trust in other Facebook users.

The theory of planned behavior variables were moderately intercorrelated. Attitudes were correlated positively with injunctive norm, descriptive norm, and perceived behavioral control. Injunctive and descriptive components of the subjective norm were intercorrelated. Despite these inter-relationships, the variables were retained as independent predictors consistent with theory and past research (Ajzen, 1991; Cialdini et al., 1991; Manning, 2009). All theory of planned behavior variables were found to correlate positively with intentions to protect privacy online. In contrast, no significant bivariate correlations were found between trust and perceived risk and intentions or T2 behavior. However, trust was positively correlated with attitudes.

Overview of Regression Analyses

A hierarchical multiple regression analysis was conducted to predict intentions, as shown in Table 2. Demographic variables of age and gender were entered in the first block, the theory of planned behavior variables (attitudes, subjective injunctive norm, subjective descriptive norm, and perceived behavioral control) in the second block, and perceived risk and trust in the third block. Secondly, a hierarchical multiple regression was conducted to predict behavior, as shown in Table 3. Demographic variables were entered in the first block, planned behavior variables including intentions in the second block, and risk and trust in the third block.

Online Privacy Protection Intentions and Behavior

Intentions. Results are summarized in Table 2. The demographics significantly explained 6% of the variance in intentions to protect privacy, $F(2,108) = 3.50$, $p = .034$. Inspection of the coefficients revealed that older participants had greater intentions to protect their privacy, $\beta = .20$, $p = .032$, $sr^2 = .04$, but no gender effects emerged, $\beta = .14$, $p = .126$, $sr^2 = .02$.

The theory of planned behavior variables accounted for an additional 27% of the variance in intentions when entered in the second block, $F_{ch}(4, 104) = 10.70$, $p < .001$. Inspection of the coefficients revealed that when participants perceived that important others approved of online privacy protection, they reported more positive intentions, $\beta = .29$, $p = .003$, $sr^2 = .06$. Furthermore, as predicted, when participants perceived that important others protected their own privacy, participants reported more positive intentions, $\beta = .27$, $p = .005$, $sr^2 = .05$. Contrary to hypotheses, intentions were not associated with attitudes, $\beta = .09$, $p = .298$, $sr^2 = .01$, or perceived behavioral control, $\beta = .12$, $p = .170$, $sr^2 = .01$.

TABLE 1
Means, Standard Deviations and Intercorrelations

Variable (scale)	M	SD	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1. Age (years)	18.91	2.99		−.01	.10	.07	.22*	.05	.06	−.15	.20*	−.04
2. Gender (−1 men, +1 women)	0.23	0.98		–	.21*	.29**	.15	.11	−.26**	.07	.14	.29**
3. Attitudes (1–7)	5.65	0.99			–	.36***	.27**	.25**	−.27**	.07	.31***	.10
4. Injunctive norm (1–7)	5.98	0.86				–	.47***	.13	−.06	−.02	.47***	.19†
5. Descriptive norm (1–7)	5.21	1.09					–	.10	−.01	.02	.47***	.00
6. Perceived behavioral control (1–7)	6.32	0.67						–	.06	−.01	.21*	.04
7. Trust (1–7)	1.90	0.99								−.09	−.03	.07
8. Perceived risk (0–1)	0.51	0.21								–	.14	−.11
9. Intentions (1–7)	5.47	1.55									–	.11
10. T2 behavior (0–22)	6.14	2.80										–

Note: $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$, $\dagger p < .10$.

TABLE 2
Hierarchical Multiple Regression Analysis of Intentions to Protect Privacy on Facebook: Block (R^2ch) and Coefficients (β)

Predictor	*Block 1*	*Block 2*	*Block 3*
Age	.20*	.10	.13
Gender	.14	−.02	−.03
Injunctive norm		.29**	.31**
Descriptive norm		.27**	.26**
Attitudes		.09	.08
Perceived behavioral control		.12	.12
Perceived risk			.17*
Trust			.00
R^2ch	.06*	.27***	.03
R^2	.06*	.34***	.36***

Note: $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

TABLE 3
Hierarchical Multiple Regression Analysis of Privacy Protection Behavior at T2: Block (R^2ch) and Coefficients (β)

Predictor	*Block 1*	*Block 2*	*Block 3*
Age	−.04	−.02	−.01
Gender	.30**	.26*	.31*
Injunctive norm		.11	.07
Descriptive norm		−.11	−.12
Attitudes		.03	.09
Perceived behavioral control		−.04	−.07
Intentions		.08	.11
Perceived risk			−.15
Trust			.15
R^2ch	.09*	.02	.04
R^2	.09*	.11	.15

Note: $^{*}p < .05$, $^{**}p < .01$.

Perceived risk and trust did not account for additional variance in intentions when entered in the third block, $F_{ch}(4, 102) = 2.08$, $p = .13$, $R^2{}_{ch} = .03$. Inspection of the coefficients revealed, however, that perceived risk was significantly positively associated with intentions to protect their privacy online, $\beta = .17$, $p = .044$, $sr^2 = .03$. Trust was not significant, $\beta < .01$, $p = .970$, $sr^2 < .01$, contrary to hypotheses.

In the final model, the variables accounted for 36% of the variance in online privacy protection intentions, $F(8, 102) = 7.19$, $p < .001$.

Behavior. As summarized in Table 3, the demographics significantly accounted for 8% of the variance in privacy protection behavior at T2, $F(2, 75) = 3.64$, $p = .031$. Gender was associated with T2 behavior, $\beta = .30$, $p = .009$, $sr^2 = .09$, such that women had higher privacy protection behavior than men. Age was not significantly associated with T2 behavior, $\beta = .04$, $p = .718$, $sr^2 < .01$.

The theory of planned behavior variables and intentions entered in the second block did not explain additional variance in T2 behavior, $F_{ch}(5, 70) = 0.32$, $p = .897$, $R^2{}_{ch} = .01$ ($|\beta s| < .11$, $ps > .431$, $sr^2s < .01$). In addition, the entry of perceived trust and risk in the third block did not explain additional variance in T2 behavior, $F_{ch}(2, 68) = 1.64$, $p = .202$, $R^2{}_{ch} = .04$; $|\beta s| < .15$, $ps > .199$, $sr^2s < .02$.

The final model accounted for 15% of the variance in T2 online privacy protection behavior, $F(9, 68) = 1.33$, $p = .236$.

DISCUSSION

The present research used an extended theory of planned behavior model that included descriptive norms, perceived risk, and trust to investigate online privacy protection in Facebook users. Results revealed that only injunctive norms, descriptive norms, and perceived risk were each a significant predictor of intentions to protect privacy online. However, only demographic variables were associated with significant variance in online privacy protection behavior after a 2-week period.

The Theory of Planned Behavior

Only the subjective injunctive and descriptive norm components of the theory of planned behavior were independently associated with intentions. When participants perceived that important others approved of online privacy protection, or perceived that important others enacted online privacy protection themselves, participants reported greater online privacy protection intentions. However, contrary to hypotheses, neither attitudes nor perceived control were unique predictors.

Although the TPB is an established and well-supported model in general, partial support for its predictions is not unusual in online behaviors (Cameron et al., 2012; Lee, 2009; Yousafzai et al., 2010). However, the particular pattern of non-significance is surprising. Past research on online privacy intentions found that attitudes and perceived control were significantly positively and independently associated with greater intentions to protect online privacy, but that the subjective norm component was non-significant (Yao & Linz, 2008; Yousafzai et al., 2010). However, other research on Facebook partner monitoring behavior found that attitude and subjective norm predicted intentions (Darvell et al., 2011). Thus, the results of the present research are unusual on two levels: the lack of statistically significant associations between attitudes and perceived control and intentions; and the novel significant associations of the subjective injunctive and descriptive norms with intentions.

At face value, the non-significant findings for attitudes and perceived control could be interpreted as indicating that these variables are unimportant in online privacy intentions and actions. However, given the significant findings for these variables in other contexts (Manning, 2009; Yousafzai et al., 2010), restriction of range due to highly positive attitudes and control may be a more likely explanation. This is particularly the case for perceived control with a mean of 6.32 (Table 1). Similarly, the non-significant association between intentions and privacy protection behavior after two weeks is inconsistent with the TPB (Ajzen, 1991) and previous meta-analyses (Armitage & Conner, 2001; Manning, 2009). One explanation may be that privacy protection in the specific context of Facebook is habitual rather than planned behavior; participants may not

change their Facebook settings at all, let alone adjust them within a 2-week window. Future research should adopt a more comprehensive set of behavioral measures, including, ideally, observation of privacy protection behavior in novel (more clearly intentional) settings.

A strength of the present study is that it used an expanded conceptualization of normative influence in the TPB by distinguishing between injunctive and descriptive norms. The results bear out the importance of doing so in the online context. While both types of norm were positive, and positively inter-correlated (Table 1), the descriptive norm was significantly less favorable to privacy protection than the injunctive norm. Moreover, both injunctive and descriptive norms were independently associated with intentions to protect privacy online, supporting the view that distinguishing these sources of normative influence allows for greater predictive power (e.g., Cialdini, 2003; Cialdini et al., 1990; Manning, 2009). The need to distinguish injunctive and descriptive components of the subjective norm may explain the failure of past research to find significant norm effects in this context (Yao & Linz, 2008). Future research into online behavior should include injunctive and descriptive norms, with an eye to discovering whether the two are always independent predictors, and whether the social network site context, and the salience of peer interactions, makes them particularly important. More broadly, the near-ubiquity of Facebook among Internet users (Internet World Stats, 2014) may shape social norms regarding online privacy protection. Facebook explicitly encourages the sharing of personal information, establishing a positive injunctive norm of disclosure (Facebook, 2014). Future work should examine the potential norm conflict (e.g., McDonald, Fielding, & Louis, 2013) between broad, Facebook-level norms that promote disclosure and specific, relevant groups (e.g., Friends) that promote privacy protection.

Roles of Perceived Risk and Trust

A final goal of the present research was to examine the role of perceived risk and trust in online privacy protection. Results revealed that perceived risk, but not trust, was associated with online privacy protection intentions: When participants perceived greater risk, they reported more positive intentions to protect their privacy online. This finding is inconsistent with Yao and Linz (2008), who did not find that risk predicted privacy protection over and above the theory of planned behavior. However, this difference might reflect the use of an implicit measure in the current study. Thus, and in line with other research, the current research suggests that there is an affective aspect in predicting intentions over and above the cognitive theory of planned behavior variables (Ajzen & Driver, 1992; French et al., 2005; Lowe et al., 2002).

There was no association found between perceived risk and actual privacy protection behavior, which may need to be measured more carefully (e.g., different online privacy behaviors may be differentially impacted by risk perceptions; see Jørgensen et al., 2013). At the same time, the finding that people's behavior neglects risk information (including expert advice) in favor of being influenced by norms is not unusual (Schmiege, Klein, & Bryan, 2010).

Trust was not associated with either privacy protection intentions or behavior. However, in line with Rotter (1980), trust was associated with attitudes to online privacy protection: those with more positive attitudes toward online privacy protection had lower trust in other Facebook users. Given that previous research has identified trust as a focal variable in determining online privacy protection, it is puzzling to find no association in the present study (Fogel & Nehmad, 2009; Metzger, 2004).

Individual Differences

In line with past research, it was found that women were marginally less trusting of other Facebook users than men, and had significantly greater privacy protection behavior than men (Fogel & Nehmad, 2009; Youn, 2009). Age was also found to be a significant predictor, such that older participants had greater intentions to protect their privacy. This is consistent with previous research suggesting that adults (compared with adolescents) disclose less information on Facebook and use the privacy settings more (Christofides et al., 2012), although in the present data, no significant unique effect of age on behavior was observed, perhaps because of restricted range (i.e., a relatively young sample).

Applied Implications

The present findings have a number of implications for online privacy protection, given that participants showed significant privacy protection deficits despite overall low levels of trust and positive attitudes to privacy protection. Broadly, the present research on privacy protection is potentially relevant to topics from willingness to disclose and support-seeking to reactions to friend requests (e.g., Greitemeyer & Kunz, 2013; Milyavskaya et al., 2010). In addition to its potential utility in marketing strategies and product development by Facebook and companies that use Facebook, such research could assist programs aimed at addressing problems such as online fraud and cyber-bullying, as well as general campaigns to promote online privacy protection. In the present data, it is clear that perceived norms are important factors in determining intentions to protect privacy on Facebook. This, combined with the lack of attitude-intention relationship, indicates that a successful privacy protection campaign must target and promote positive injunctive and descriptive norms of online privacy protection. A successful campaign must be aware that discrepancies between what important others approve of and what important others actually do may undermine the effectiveness of a normative message (see also McDonald, Fielding, & Louis, 2012; 2013; Smith et al., 2012). A campaign that highlights the negative consequences of failing to protect privacy may also be especially effective by increasing individuals' perceptions of risk.

At the same time, it should be acknowledged that Facebook privacy needs are subjective: Many people may believe that they already have sufficiently high privacy protection levels and may not have seen the clear value in increasing their privacy levels (and, indeed, privacy needs may vary according to the content of an individual's Facebook profile). It is possible that our participants were insufficiently aware of the negative consequences of not increasing their privacy settings (particularly so since Facebook gives clear options for levels of privacy). In other contexts (e.g., health), people may be more readily aware of what kinds of behaviors are likely to be beneficial. It is reasonable, then, to expect TPB variables to predict more clearly intentions and behavior in such contexts.

General Limitations and Future Directions

The present work was broadly successful in its core aim of investigating online privacy protection behavior using a theoretically integrative approach. However, several general limitations of the current research must be acknowledged. Strong causal inferences cannot be drawn from

the correlational—rather than experimental—research design of the present work. Although data were collected at two time points, significant associations were only found between variables measured at the first time point (e.g., subjective norm, perceived risk, intentions to protect privacy online), and not at the second time point (actual privacy protection behavior). Future research could investigate additional variables at the second time point, and could take a more experimental approach to investigating the role of TPB in predicting online privacy protection behavior.

Other limitations include the use of a convenience sample and self-report methodology. A university student sample may not show the same level or pattern of influences of online privacy protection behavior as the general population, given that adolescents generally spend more time and disclose more information on Facebook than older adults (Christofides et al., 2012). Similarly, our self-report measure of online privacy protection intentions may not accurately represent participants' behavior, given the potential social desirability of appearing cautious despite being careless with one's online privacy.

The lack of any significant association between trust or risk and privacy protection intentions or behavior may be due to problems with the measures. Specifically, the trust target was specified as "all Facebook users." For example, participants were asked their agreement with the statement "I trust all Facebook users," This may have prompted more negative responses due to participants focusing on the fact that not *all* Facebook users are trustworthy (even if only a small few are not), or that the label may have been seen to include widely distrusted groups, such as criminal hackers or even the Facebook company itself. This possibility is supported by the low observed mean for trust: 1.90 ($SD = 0.99$) on the 1–7 scale. This floor effect may have led to an underestimation of its previously established association with privacy protection intentions and behavior (Christofides et al., 2012). A more useful measure of trust might have been trust in one's own Facebook network or *most* Facebook users. In addition, the use of a scale of only two items may have compromised its reliability. Use of a multi-item established scale from the literature (e.g., Dunn & Schweitzer, 2005) may ameliorate this issue; future research into online privacy protection should include such a scale. Future research should also consider more carefully the measurement of risk, given our finding that risk predicted intentions but not behavior. For example, both implicit and explicit perceived-risk measures could be included, and the differences between the two types of risk perceptions explored. Other factors that have been found to predict behavior over and above the theory of planned behavior include affective variables such as positive and negative anticipatory emotions (e.g., Kobbeltvedt & Wolff, 2009; Rivis, Sheeran, & Armitage, 2009). The present research did not include any emotion measures, and future research could examine whether these uniquely predict privacy protection over and above the variables examined in the present work.

Conclusion

The core ambition of the present study was to integrate a number of theoretical approaches for investigating online privacy protection, including the theory of planned behavior, norm focus theory, and affective variables previously linked to privacy protection such as perceived risk and trust. As such, it is somewhat unsurprising that the study yielded mixed results. Support was found for norm focus theory and the importance of distinguishing the independent effects of subjective injunctive and subjective descriptive norms in predicting intentions. Indeed, far from being weak predictors of behavior, as in some previous TPB research (e.g., Yao & Linz, 2008), subjective

norms were the only TPB variables that predicted privacy protection intentions. This suggests, then, that previous online privacy research may have neglected a significant role of injunctive and descriptive norms in online privacy protection. The unique role of perceived risk in predicting intentions over and above the theory of planned behavior is consistent with those who have argued that planned behavior variables may not capture variance associated with emotions and affective attitudes (Ajzen & Driver, 1992; French et al., 2005; Lowe et al., 2002). At the same time, the referent group or target for trust, and the role of trust itself, are in need of more theoretical attention. Trust in depersonalized other users of a social media platform was considered here. However, risk perceptions and trust in relation to company behavior could be important in understanding online privacy protection, as when changes in policy and default settings by Facebook itself change privacy implications radically without explicit participant action.

Without overinterpreting the available data, it is clear that not all specified predictors have unique contributions to privacy protection intentions. If the findings of the present study are replicated, it could be tentatively concluded that subjective norms and perceived risk are more important determinants of online privacy protection than attitudes, perceived behavioral control, or trust.

Intentions also were found not to generalize to behavior in this context, which is an important warning for the privacy protection literature, and consistent with the warnings of some security experts that individuals often fail to update and change their security settings (Furnell, 2005). A focus on the occasions when participants update their privacy protection, and on novel contexts when participants first engage with organizations and networks, may thus be warranted in future research seeking to examine intentional privacy behavior online.

The present study is an important first step in gaining a more complete understanding of individuals' privacy protection behavior. Further research is required so that effective interventions to promote privacy protection may be developed and implemented in a world where privacy is increasingly under threat.

AUTHOR NOTES

Alexander K. Saeri is a PhD Candidate in the School of Psychology at the University of Queensland. His research interests include collective action, social change, and the influence of social identity and norms on critical and scientific thinking. **Claudette Ogilvie** is affiliated with the School of Psychology at the University of Queensland. **Stephen T. La Macchia** is a PhD Candidate in the School of Psychology at the University of Queensland. His main research interests are trust, implicit theories of group processes and contact, and factors affecting group-based morality. **Joanne R. Smith** is a Senior Lecturer in the School of Psychology at the University of Exeter. Her research interests include the impact of social identity and norms on behavior change, particularly in the domains of health and environmental behavior. **Winnifred R. Louis** is an Associate Professor in the School of Psychology at the University of Queensland. Her research interests focus on the influence of identity and norms on social decision-making.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I. (2006). *Constructing a TPB questionnaire: Conceptual and methodological considerations*. Retrieved from http://www.people.umass.edu/aizen/pdf/tpb.measurement.pdf

Ajzen, I., & Driver, B. L. (1992). Application of the theory of planned behavior to leisure choice. *Journal of Leisure Research*, *24*, 207–224.

Alter, A. L., & Oppenheimer, D. M. (2009). Suppressing secrecy through metacognitive ease. *Psychological Science*, *20*, 1414–1420. doi:10.1111/j.1467-9280.2009.02461.x

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology*, *40*, 471–499. doi:10.1348/014466601164939

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x

Cameron, R., Ginsburg, H., Westhoff, M., & Mendez, R. V. (2012). Ajzen's theory of planned behavior and social media use by college students. *American Journal of Psychological Research, 18*(1), 1–20. Retrieved from: http://www.mcneese.edu/ajpr/

Christofides, E., Muise, A., & Desmarais, S. (2012), Hey Mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, *3*(1), 48–54. doi:10.1177/1948550611408619

Chudry, F., Foxall, G., & Pallister, J., (2011). Exploring attitudes and predicting intentions: Profiling student debtors using an extended theory of planned behavior. *Journal of Applied Social Psychology*, *41*(1), 119–149. doi:10.1111/j.1559-1816.2010.00705.x

Cialdini, R. B., (2003). Crafting normative messages to protect the environment. *Current Directions in Psychological Science*, *12*, 105–109. doi:10.1111/1467-8721.01242

Cialdini, R. B., Demaine, L. J., Sagarin, B. J., Barrett, D. W., Rhoads, K., & Winter, P. L., (2006). Managing social norms for persuasive impact, *Social Influence*, *1*(1), 3–15. doi:10.1080/15534510500181459

Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A focus theory of normative conduct: A theoretical refinement and re-evaluation of the role of norms in human behavior. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 24, pp. 201–233). San Diego, CA: Academic Press.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*, *58*, 1015–1026. doi:10.1037/0022-3514.58.6.1015

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, *79*(2), 73–91. doi:10.1037/h0033950

Darvell, M. J., Walsch, S. P., & White, K. M., (2011). Facebook tells me so: Applying the theory of planned behavior to understand partner-monitoring behavior on Facebook. *Cyberpsychology, Behavior and Social Networking*, *14*(12), 717–722. doi:10.1089/cyber.2011.0035.

D'Astous, A., Colbert, F., & Montpetit, D. (2005). Music piracy on the web—How effective are anti-piracy arguments? *Journal of Consumer Policy*, *28*, 289–310. doi:10.1007/s10603-005-8489-5

Duncan, E. M., Forbes-McKay, K., & Henderson, S. E., (2012). Alcohol use during pregnancy: An application of the theory of planned behavior. *Journal of Applied Social Psychology 42*, 1887–1903. doi:10.1111/j.1559-1816.2012.00923.x

Dunn, J. R., & Schweitzer, M. E. (2005). Feeling and believing: The influence of emotion on trust. *Journal of Personality and Social Psychology*, *88*, 736–748. doi:10.1037/0022-3514.88.5.736

Electronic Frontiers Australia (2006). *EFA—Privacy and surveillance*. Retrieved from http://www.efa.org.au/privacy/

Facebook. (2014). *Facebook—About*. Retrieved from https://www.facebook.com/facebook/info

Foddy, M., Platow, M. J., & Yamagishi, T. (2009). Group-based trust in strangers. *Psychological Science*, *20*, 419–422. doi:10.1111/j.1467-9280.2009.02312.x

Fogel, J., & Nehmad, E. (2009). Internet social communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*, 153–160. doi:10.1016/j.chb.2008.08.006

French, D. P., Sutton, S., Hennings, S. J., Mitchell, J., Wareham, N. J., Griffin, S., . . . Kinmonth, A. L. (2005). The importance of affective beliefs and attitudes in the theory of planned behavior: Predicting intentions to increase physical activity. *Journal of Applied Social Psychology*, *35*, 1824–1848. doi:10.1111/j.1559-1816.2005.tb02197.x

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*, 274–279. doi:10.1016/j.cose.2005.04.003

Greitemeyer, T., & Kunz, I. (2013). Name-valence and physical attractiveness in Facebook: Their compensatory effects on friendship acceptance. *Journal of Social Psychology*, *153*, 257–260. doi:10.1080/00224545.2012.741629

Henderson, S., & Gilding, M. (2004). "I've never clicked this much with anyone in my life": Trust and hyperpersonal communication in online friendship. *New Media and Society*, *6*, 487–506. doi:10.1177/146144804044331

Internet World Stats. (2014). *Internet usage statistics*. Retrieved from http://www.internetworldstats.com/stats.htm

Jørgensen, Ø., Bäckström, M., & Björklund, F. (2013). Bidirectional correction in social judgments: How a cue to the risk of bias causes more favorable ratings of some groups but less favorable of others. *Journal of Social Psychology*, *153*, 131–148. doi:10.1080/00224545.2012.711382

Karimi-Shahanjarini, A., Rashidian, A., Majdzadeh, R., Omidvar, N., Tabatabai, M., & Shojaeezadeh, D., (2012), Parental control and junk-food consumption: A mediating and moderating effect analysis. *Journal of Applied Social Psychology*, *42*, 1241–1265. doi:10.1111/j.1559-1816.2011.00885.x

Kenworthy, J. B., & Jones, J. (2009). The roles of group importance and anxiety in predicting depersonalized ingroup trust. *Group Processes and Intergroup Relations*, *12*, 227–239. doi:10.1177/1368430208101058

Knowles, S. R., Hyde, M. K., & White, K. M., (2012). Predictors of young people's charitable intentions to donate money: An extended theory of planned behavior perspective. *Journal of Applied Social Psychology 42*, 2096–2110. doi:10.1111/j.1559-1816.2012.00932.x

Kobbeltvedt, T., & Wolff, K. (2009). The risk-as-feelings hypothesis in a theory-of-planned-behavior perspective. *Judgment and Decision Making*, *4*, 567–586.

Lee, M. (2009). Predicting and explaining the adoption of online trading: An empirical study in Taiwan. *Decision Support Systems*, *47*, 133–142. doi:10.1016/j.dss.2009.02.003

Ling, I.-L., Chuang, S.-C., & Hsiao, C. H. (2012). The effects of self-diagnostic information on risk perception of Internet addiction disorder: Risk perception of Internet addiction disorder: Self-positivity bias and online social support. *Journal of Applied Social Psychology*, *42*, 2111–2136. doi:10.1111/j.1559-1816.2012.00933.x

Louis, W. R., Davies, S., Terry, D. J., & Smith, J. R. (2007). Pizza and pop and the student identity: The role of referent group norms in healthy and unhealthy eating. *Journal of Social Psychology*, *147*, 57–74. doi:10.3200/SOCP.147.1.57-74

Lowe, R., Eves, F., & Carroll, D. (2002), The influence of affective and instrumental beliefs on exercise intentions and behavior: A longitudinal analysis. *Journal of Applied Social Psychology*, *32*, 1241–1252. doi:10.1111/j.1559-1816.2002.tb01434.x

Manning, M. (2009). The effects of subjective norms on behavior in the theory of planned behavior: A meta-analysis. *British Journal of Social Psychology*, *48*, 649–705. doi:10.1348/014466608X393136

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59*, 411–429. doi:10.1111/1540-4560.00071

McCabe, M., & Ricciardelli, L. (2003). Sociocultural influences on body image and body changes among adolescent boys and girls. *Journal of Social Psychology*, *143*(1), 5–26. doi:10.1080/00224540309598428

McDonald, R. I., Fielding, K. S., & Louis, W. R. (2012). Conflicting norms highlight the need for action. *Environment and Behavior, 46*(2), 139–162. doi:10.1177/0013916512453992

McDonald, R. I., Fielding, K. S., & Louis, W. R. (2013). Energizing and de-motivating effects of norm conflict. *Personality and Social Psychology Bulletin*, *39(1)*, 57–72. doi:10.1177/0146167212464234

McLachlan, S., & Haggar, M. S., (2011). The influence of chronically accessible autonomous and controlling motives on physical activity within an extended theory of planned behavior. *Journal of Applied Social Psychology, 41*, 445–470. doi:10.1111/j.1559-1816.2010.00721.x

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. Journal of *Computer-Mediated Communication, 9*(4). doi:10.1111/j.1083-6101.2004.tb00292.x

Milyavskaya, M., Reoch, J., Koestner, R. F., & Losier, G. F. (2010). Seeking social connectedness: Interdependent self-construal and impression formation using photographic cues of social connectedness. *Journal of Social Psychology*, *150*, 689–702. doi:10.1080/00224540903365406

Nolan, J. P., Schultz, P. W., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2008). Normative social influence is underdetected. *Personality and Social Psychology Bulletin*, *34*, 913–923. doi:10.1177/0146167208316691

Paine, C., Reips, U-D., Steiger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International journal of Human-Computer Studies*, *65*, 526–536. doi:10.1016/j.ijhcs.2006.12.001

Rivis, A., Sheeran, P., & Armitage, C. J. (2009). Expanding the affective and normative components of the theory of planned behavior: A meta-analysis of anticipated affect and moral norms. *Journal of Applied Social Psychology*, *39*, 2985–3019. doi:10.1111/j.1559-1816.2009.00558.x

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, *35*(1), 1–7. doi:10.1037/0003-066X.35.1.1

Schmiege, S. J., Bryan, A., Klein, W. M. P., (2009). Distinctions between worry and perceived risk in the context of the theory of planned behavior. *Journal of Applied Social Psychology 39*(1), 95–119. doi:10.1111/j.1559-1816.2008.00431.x

Schmiege, S. J., Klein, W. M. P., & Bryan, A. D. (2010). The effect of peer comparison information in the context of expert recommendations on risk perceptions and subsequent behavior. *European Journal of Social Psychology*, *40*, 746–759. doi:10.1002/ejsp.645

Schofield, C. B., & Joinson, A. N. (2008). Privacy, trust, and disclosure online. In E. Barak (Ed.), *Psychological aspects of cyberspace: Theory, research, applications* (pp. 13–31). Cambridge, UK: Cambridge University Press.

Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behavior relationship. *British Journal of Social Psychology*, *47*, 647–666. doi:10.1348/014466607X269748

Smith, J. R., Louis, W. R., Terry, D. J., Greenaway, K. H., Clarke, M. R., & Cheng, X. (2012). Congruent or conflicted? The impact of injunctive and descriptive norms on environmental intentions. *Journal of Environmental Psychology*, *32*, 353–361. doi:10.1016/j.jenvp.2012.06.001

Smith, J. R., Terry, D. J., Manstead, A. S., Louis, W. R., Kotterman, D., & Wolfs, J. (2008). The attitude–behavior relationship in consumer conduct: The role of norms, past behavior, and self-identity. *The Journal of Social Psychology*, *148*, 311–334. doi:10.3200/SOCP.148.4.473-492

Sparck-Jones, K. (2003). Privacy: What's different now? *Interdisciplinary Science Reviews*, *28*, 287–292. doi:10.1179/030801803225008677

Wang, Y. D. & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105–125. doi:10.1016/j.chb.2003.11.008

Whitty, M. T., & Joinson, A. N. (2008). Truth, lies, and trust on the Internet. London, UK: Routledge.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior*, *11*, 615–616. doi:10.1089/cpb.2007.0208.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs, 43*, 389–418. doi:10.1111/j.1745-6606.2009.01146.x

Youn, S. & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior*, *11*, 763–765. doi:10.1089/cpb.2007.0240

Yousafzai, S. Y., Foxall, G. R., & Pallister, J. G. (2010). Explaining Internet banking behavior: Theory of reasoned action, theory of planned behavior, or technology acceptance model? *Journal of Applied Social Psychology*, *40*, 1172–1202. doi:10.1111/j.1559-1816.2010.00615.x

Received August 19, 2013
Accepted April 10, 2014