Predicting Facebook users’ online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior

Alexander K. Saeri, Claudette Ogilvie, and Stephen La Macchia
The University of Queensland, Australia

Joanne R. Smith
The University of Exeter, United Kingdom

Winnifred R. Louis
The University of Queensland, Australia

This version updated 3 November 2013

The present research adopts an extended theory of 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 two 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 were no unique effects of trust on intentions, or of risk or trust on behavior.

Keywords: theory of planned behavior, group norms, Facebook, online privacy

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, 2012). 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). 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 all the internet, 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 victimisation (McCabe & Ricciardelli, 2003). Individuals’ calibration of their disclosure thus may have important applied consequences, positive as well as negative. More broadly, the ex-
plosive 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 present research aims to contribute to the growing body of research addressing online social networking sites and online social behaviour.

On a theoretical level, the present research aims to make three specific contributions: adding to the growing body of research applying the theory of planned behaviour to decision-making in cyberspace; providing the first independent test of norm focus theory (Cialdini, Kallgren, & Reno, 1991) in online privacy protection by examining the independent roles of subjective injunctive and subjective descriptive norms; and contributing to research on affect in relation to the theory of planned behaviour by examining the roles of trust and risk in relation to each other and to the other models.

The Theory of Planned Behavior

The theory of planned behavior (TPB) is a robust and flexible conceptual framework that allows researchers to predict whether an individual will perform a given behavior by examining their intentions to perform that behavior (Ajzen, 1991). These intentions, in turn, are predicted by attitudes towards the behavior, subjective norms regarding the behavior and perceived control over the behavior. Within the context of the theory of planned behaviour, an attitude is the evaluation of an outcome of a given behavior as positive or negative. Subjective norms refer to perceived social pressure from important others to engage or not engage in the behavior. Subjective norm and perceived behavioral control each uniquely predict intentions to perform a given behavior, and intentions directly predict that behavior.

The theory of planned behaviour has demonstrated efficacy as a conceptual framework for examining the antecedents of behaviors and affecting behavior change. The model has been used to examine a range of health behaviors (Duncan, Forbes-McKay, & Henderson, 2012; Karimi-Shahjari, Louis, Davies, Smith, & Terry, 2007), socially-minded behaviors such as energy conservation (Nolan, Schultz, Cialdini, Goldstein, & Griskevicius, 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 online music piracy (d’Astous, Colbert, & Montpetit, 2005), partner monitoring behavior on Facebook (Darvell, Walsch & White, 2011), online stock trading (Lee, 2009), and online privacy protection (Yao & Linz, 2008; Yousafzai et al., 2010). In the domain of online privacy protection, research has generally supported the role of attitudes and intentions as predictors of behavior, with less support for the role of norms (Yousafzai et al., 2010). However, this research has also considered the role of affective variables, such as fear of crime (Yao & Linz, 2008) or trust (Yousafzai et al., 2010), illustrating that additional factors may be important in this context. The current study extends previous work by examining online privacy protection in the context of social network services and social media, an emerging nexus of research and applied concern. We also aim to distinguish the role of injunctive and descriptive norms in this context for the first time, and to test the independent contributions of risk and trust, as elaborated below.

Injunctive and Descriptive Norms

Although the theory of planned behaviour is a robust and efficacious framework for investigating antecedents of behaviour, 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 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, 2003; Cialdini, Reno, & Kallgren, 1990; Cialdini et al., 2006; Jacobson, Mortenson, & Cialdini, 2011). Thus, social influence will be underestimated if researchers fail to conceptualise 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: 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. However, no research to date has considered the independent effects of injunctive and descriptive norms for online privacy behavior.

Risk and Trust

The theory of planned behavior can be considered as 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 criticised by some researchers, who have called for the inclusion of affective variables within the model (e.g., Ajzen & Driver, 1992; French et al., 2005; 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 role of risk.** Risk perceptions are important cues in social judgements (JÃÿrgensen, BÃd'ckstrÃ˝ um, & BjÃ˝ urk-lund, 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, it should be noted that past research on the relationship of risk and online privacy protection behavior may have confounded perceived risk with attitudes to privacy protection. That is, in the context of online privacy, risk is typically conceptualised as “privacy concerns”, and assessed with items such as “Do you have any concerns about your privacy while you are using the internet?” (Paine et al., 2007). To address this issue, we measure implicit perceived risk using a word-stem completion task (see Alter & Oppenheimer, 2009).

**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, & Hsiao, 2012). However, trust also extends beyond interpersonal relationships: trust in a commercial organisation encourages disclosure of personal information (Metzger, 2004; Whitty & Joinson, 2008).

Recent research into online privacy have found a negative association between trust and privacy protection; however, these studies have focused primarily on trust between a consumer and business (see Wang & Emurian, 2005, for a review). In the context of a social networking site such as Facebook, salient relationships are of an interpersonal rather than consumer nature. Base levels of trust may be higher than found in previous research (see Wang & Emurian, 2005), as individuals tend to trust other individuals more than commercial businesses (Christofides et al., 2012; Metzger, 2004). Nevertheless, research has found higher trust to be associated with less protective Facebook privacy settings (Christofides et al., 2012), particularly among adolescents.

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 a group as well as at an interpersonal level, with individuals trusting members of groups they belong to (ingroup) more than members of groups they don’t belong to (outgroup; e.g., Foddy, Platow, & Yamagishi, 2009) â ˘A¸ S a concept known as “de-personalised ingroup trust”. By default, personal information disclosed on a Facebook profile is available to Friends (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 the personal information disclosed on his or her profile. 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, the concept of depersonalised ingroup trust becomes increasingly relevant. In the present study, the association between depersonalised ingroup trust of Facebook users and online privacy protection intentions and behaviour is investigated.

**Control variables**

Past research has suggested that gender differences exist in online privacy protection (Youn, 2009), such that men are less likely to protect their privacy than women (Fogel & Nehmad, 2009). In addition, previous research has found that age is associated with online privacy protection, such that adults (compared with adolescents) disclosed less information on Facebook, and used the privacy settings more (Christofides et al., 2012). For these reasons, age and gender were included as measured control variables in the present research.

**The present study**

The present study has three theoretical objectives: to investigate online privacy protection behavior within the framework of a major decision making model, the theory of planned behavior; to examine the role of normative influence in online privacy protection while distinguishing between injunctive and subjective descriptive norms; and to test the direct associations of perceived risk and trust with online privacy protection.

In fulfilling these aims, the current study makes a number of important contributions. It is the first study to distinguish between injunctive and descriptive norms when examining online behaviour in the framework of the theory of

**IDEOLOGY AND COLLECTIVE ACTION**

The present study has three theoretical objectives: to investigate online privacy protection behavior within the framework of a major decision making model, the theory of planned behavior; to examine the role of normative influence in online privacy protection while distinguishing between injunctive and subjective descriptive norms; and to test the direct associations of perceived risk and trust with online privacy protection.

In fulfilling these aims, the current study makes a number of important contributions. It is the first study to distinguish between injunctive and descriptive norms when examining online behaviour in the framework of the theory of
planned behavior. Second, it employs an implicit measure of perceived risk, in order to reduce confounds associated with “privacy concerns” scales (Youn, 2009; Youn & Hall, 2008). Further, a self-report measure of online privacy protection behavior is included, measured longitudinally, two weeks following the study. Finally, the present research examines the roles of perceived risk and trust on online privacy protection intentions and behaviour in relation to the theory of planned behavior, testing the hypothesis that they would play a direct role over and above the theory of planned behavior variables.

In line with previous research (d’Astous et al., 2005; Darvell, Walsh, & White, 2011; Yousafzai et al., 2010), it is hypothesised that attitudes, subjective injunctive norm, subjective descriptive norm, and perceived behavioural control will all be positively associated with intentions to protect privacy online. It is also predicted that intentions will be positively associated with online privacy protection behavior. However, it is expected that greater perceived risk and greater trust will independently be associated with stronger intentions to protect privacy, and that they will predict privacy protection over and above the theory of planned behavior.

Method

Participants

A convenience sample of 119 first-year psychology students from an Australian university participated in return for partial course credit. Participants volunteered for the study using a web-based system, where the study was advertised as “Facebook users’ attitudes towards online privacy”. Current Facebook membership was a prerequisite for participation in the study. 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 behaviour measured two weeks following the study (T2 behaviour) served as dependent measures. The theory of planned behaviour variables (attitudes, subjective injunctive norm, subjective descriptive norm, and perceived behavioural control) were also measured, as were age and gender. Two additional variables were included as potential independent predictors of the relationship between the theory of planned behaviour and the dependent variables: perceived risk, and trust of other Facebook users. Procedure

The study was conducted in an internet-connected laboratory in groups of up to ten. 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 behaviour variables (intentions, attitudes, injunctive and subjective descriptive norms, and perceived behavioural control), and age and gender. Two free-response items were used to probe for suspicion of study hypotheses (i.e., “What do you think this study was about?” and “What do you think the hypotheses were?”).

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 two weeks. Most (N = 107, 96)

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 fifteen word-stems. Eight of the word-stems could be completed to form risk-related words (e.g., “threa_” could be completed as “threat”, or “thread”). 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. A two-item measure adapted from previous research (Kenworthy & Jones, 2009) was 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”; 1, strongly agree, to 7, strongly disagree). Items were averaged to form a scale with higher scores indicating greater trust (İs = .61).

Attitudes. Participants’ attitudes toward protecting their privacy online were assessed using five semantic differential items adapted from Ajzen (2006). 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”: 1, worthless, to 7, valuable). Two items were reverse-scored (e.g., 1, pleasant, to 7, unpleasant). Items were averaged to form a scale with higher scores indicating more positive attitudes toward online privacy protection (İs = .82).
**Subjective injunctive norm.** Interpersonal subjective injunctive norms toward online privacy protection were assessed with a four-item measure adapted from previous 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”: 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”: 1, should, to 7, should not). Scores on the items were averaged to form a scale, with higher scores indicating a more positive subjective injunctive norm (Ƞ² = .65).

**Subjective descriptive norm.** Interpersonal subjective descriptive norms toward online privacy protection were assessed with a four-item measure derived from previous 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”: 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”: 1, protect, to 7, not protect). Scores on the items were averaged to form a scale, with higher scores indicating a more positive subjective descriptive norm (Ƞ² = .69).

**Perceived behavioral control.** Perceptions of control over online privacy protection behavior were assessed using a four-item measure adapted from previous research (Ajzen, 2006). Items were rated on a 7-item 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”: 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”: 1, very easy, to 7, very difficult). Items were averaged to form a scale, with high scores indicating greater perceived behavioral control (Ƞ² = .63).

**Intentions.** A four-item measure adapted from previous research (Ajzen, 2006) 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”: 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”: 1, completely true, to 7, completely false). Items were averaged to form a scale, with higher scores indicating greater intentions to engage in online privacy protection (Ƞ² = .91).

**Behavior.** A researcher searched for consenting participants’ profiles on Facebook using information provided. The researcher recorded whether a participant disclosed 22 types of personal information, including profile photo, interests, birthday, current location, email, etc. The behavior measure was recorded 14 days following the first session (i.e., once participants had the opportunity to enact any online privacy protection behavior changes intended after participating in the study). The total number of items of disclosed information (out of 22) was reverse-coded so that higher scores indicated greater privacy protection behavior. (Unfortunately only the total was noted; in retrospect, it would have been interesting to distinguish subsets or gradations of more intimate disclosure.)

**Demographics and suspicion.** Participants indicated their age in years, and gender (coded as -1 = men, +1 = women). Suspicion was assessed with two open-ended questions (e.g., “What do you think the hypotheses were?”). As described previously, participants who guessed the true purpose of the study were excluded from analyses.

**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 behavioural 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 (Ƞ²[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 interrelationships, 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 behaviour. 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 at Block 1, the theory of planned behavior variables (attitudes, subjective injunctive norm, subjective descriptive norm, and perceived behavioral control) at Block 2, and perceived risk and trust in Block 3. Secondly, a hierarchical multiple regression was conducted to predict behavior, as shown in Table 3. Demographic variables were entered at Block 1, planned behavior variables including intentions at Block 2, and risk and trust at Block 3.

**Online privacy protection intentions and behavior**

**Intentions.** Results are summarised 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 at Block 2, $F_{ch}(4, 104) = 10.70, p < .001$. 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, $\beta = .12, p = .170, sr^2 = .01$.

Perceived risk and trust did not account for additional variance in intentions when entered at Block 3, $F_{ch}(2, 102) = 2.08, p = .130, R^2_{ch} = .03$. 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 summarised in Table 3, the demographics significantly accounted for 9% 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 behaviour than men. Age was not significantly associated with T2 behavior, $\beta = -.04, p = .718, sr^2 < .01$.

The theory of planned behaviour variables and intentions entered at Block 2 did not explain additional variance in T2 behaviour, $F_{ch}(5, 70) = 0.32, p = .897, R^2_{ch} = .02; |\beta| < .11, ps > .431, sr^2s < .01$. In addition, the entry of perceived trust and risk at Block 3 did not explain additional variance in T2 behaviour, $F_{ch}(2, 68) = 1.64, p = .202, R^2_{ch} = .04; |\beta| < .15, ps > .199, sr^2s < .02$.

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

**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 significant predictors of intentions to protect privacy online. However, only demographic variables were associated with significant variance in online privacy protection behavior after a two 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 behaviours (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 behaviour 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 behaviour 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 behaviour; once set, participants may not change their Facebook privacy settings at all, let alone adjust them within a two-week window. Future research should adopt a more comprehensive set of behavioural measures, including ideally observation of behaviour in novel (more clearly intentional) settings.

A strength of the present study is that it used an expanded conceptualisation 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 favourable 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 behaviour 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.

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 behaviour. 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 behaviour variables (Ajzen & Driver, 1992; French et al., 2005; Lowe et al., 2002).

There was no association found between perceived risk and actual privacy protection behaviour, 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 behaviour neglects risk information (including expert advice) in favour of being influenced by norms is not unusual (Schmiege, Klein, & Bryan, 2010).

Trust was not associated with either privacy protection intentions or behaviour. However, in line with Rotter (1980), trust was associated with attitudes to online privacy protection: those with more positive attitudes towards 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). It is likely that the decision to conceptualise the relevant trust target of “all Facebook users” is the culprit here. Participants’ trust issues in this context may centre around criminal hackers, or even the company itself. A more relevant measure of trust might have been trust in their own Facebook network or even internet users in general (given that what was measured behaviourally was number of items disclosed to strangers).

Future research should also consider more carefully the measurement of risk, for example by including both implicit and explicit perceived risk measures, and exploring the differences between the two types of risk perceptions. In addition, the measurement of trust in relevant referent group targets must be highlighted as a limitation of the present study and improved in future research on this topic.

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 behaviour than men (see also 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 behaviour 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. More
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 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, in press; Smith et al., 2012; Staunton et al., in press). 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. These people may have seen no value in increasing their privacy levels. Indeed, the optimal level of privacy for a Facebook user is likely to vary according to the type of content on their Facebook profile. Furthermore, it is possible that our participants were insufficiently aware of negative consequences that may result if they choose not to increase their privacy levels. In other contexts (e.g., health), people may be more readily aware of what kinds of behaviours are likely to be beneficial or detrimental. We therefore would expect TPB variables to predict more clearly intentions and behavior in such contexts.

Conclusion

The present research adopted an extended theory of planned behaviour framework to examine online privacy protection. Results suggest that previous online privacy research may have neglected a significant role of injunctive and descriptive norms in online privacy protection. Intentions also were found not to generalise to behaviour 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 the organisations and networks, may thus be warranted in future research seeking to examine intentional privacy behaviour online. In addition, a unique role for risk in predicting intentions over and above the theory of planned behaviour is consistent with those who have argued that planned behaviour 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 depersonalised other users of a social media platform was considered here. However, risk perceptions and trust in relation to company behaviour could be important in understanding online privacy protection, as when changes in policy and default settings change privacy implications radically without explicit participant action.

The present study is an important first step in gaining a more complete understanding of individuals’ privacy protection behaviour. 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.

References


location, 3 December 2012.


