



Predicting online privacy protection for Facebook users with an extended theory of planned behavior

Mustafa Biber, Winnifred R Louis & Joanne R Smith

To cite this article: Mustafa Biber, Winnifred R Louis & Joanne R Smith (21 Feb 2024): Predicting online privacy protection for Facebook users with an extended theory of planned behavior, The Journal of Social Psychology, DOI: [10.1080/00224545.2024.2319177](https://doi.org/10.1080/00224545.2024.2319177)

To link to this article: <https://doi.org/10.1080/00224545.2024.2319177>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 21 Feb 2024.



[Submit your article to this journal](#)



[View related articles](#)



[View Crossmark data](#)



This article has been awarded the Centre for Open Science 'Preregistered' badge.



This article has been awarded the Centre for Open Science 'Open Data' badge.



This article has been awarded the Centre for Open Science 'Open Materials' badge.

Predicting online privacy protection for Facebook users with an extended theory of planned behavior

Mustafa Biber^a, Winnifred R Louis^b, and Joanne R Smith^a

^aUniversity of Exeter; ^bUniversity of Queensland

ABSTRACT

The current research uses an extended theory of planned behavior (TPB) model to predict Facebook users' ($N = 376$) intentions to protect their privacy online. It aims to replicate and extend Saeri et al. (2014) who found partial support for an extended TPB model that included descriptive norms, perceived risk, and trust. Facebook users completed an online questionnaire assessing attitudes, norms (subjective and group), perceived behavioral control (PBC), perceived risk, trust, privacy concerns, and intentions to protect their privacy online. Results revealed that attitudes, subjective norms, and PBC (i.e. the TPB) predicted online privacy intentions, as well as descriptive group norms and privacy concerns. However, perceived risk, trust, and injunctive group norms were not significant unique predictors of online privacy intentions. The implications for understanding influences on individuals' willingness to protect their privacy online are discussed.

ARTICLE HISTORY

Received 19 December 2022
Accepted 12 February 2024



KEYWORDS

Facebook; online privacy;
theory of planned behavior

Introduction

There are over 5,385 billion active internet users (Internet World Stats, 2023). Engagement with social media platforms is one of the most common uses of the internet (Statista Research Department, 2019), and one that has only increased during the COVID-19 pandemic (Nabity-Grover et al., 2020). Facebook is a popular social network that aims to foster communication between people and exchange information. As of the fourth quarter of 2023, it had approximately 2.98 billion active users monthly making it the largest social network in the world (Statista Research Department, 2023). Despite its popularity, Facebook has been involved in several scandals, which have led to user-led campaigns to reduce its influence (e.g., #deleteFacebook) and political inquiries as to its influence.

One of the most significant scandals involving Facebook was the Cambridge Analytica scandal in 2018, in which the data of around 87 million people was harvested without their consent (Graham-Harrison & Cadwalladr, 2018). It might be expected that these events would increase individuals' online data privacy concerns (Tuttle, 2018). However, individuals often do not take action to protect their privacy in the wake of data breaches (Choi et al., 2018) or even behave in ways that conflict with expressed privacy concerns (e.g., Barnes, 2006; Norberg et al., 2007). To date, there has been little research that has examined Facebook users' privacy protection intentions post-Cambridge Analytica scandals (cf. Hinds et al., 2020), and the available research has tended to focus primarily on privacy concerns (e.g., Brown, 2020) at the expense of other variables that have been found to predict Facebook privacy (Saeri et al., 2014), such as attitudes, subjective norms, perceived behavioral control (PBC), perceived trust, and risk. The present research adopts an extended Theory of Planned Behavior model, which includes privacy concerns and group norms, to provide a better understanding of Facebook privacy protection intentions.

CONTACT Mustafa Biber  mb933@exeter.ac.uk  School of Psychology, University of Exeter, Washington Singer Building, Perry Road, Exeter EX4 4QG, UK

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

The theory of planned behavior

According to the TPB (Ajzen, 1991), the most proximal determinant of behavior is the individual's intention to engage in that behavior. Intentions, in turn, are predicted by attitudes, subjective norms, and perceived behavioral control (PBC). In the context of the TPB, an attitude is defined as a positive or negative evaluation of the behavior (Ajzen, 1991; Fishbein & Ajzen, 2010). Subjective norm is defined as the extent to which important others would approve of the behavior. Finally, PBC is the individual's perceptions of the ease or difficulty of performing the behavior. There is strong support for the TPB and its ability to explain a wide variety of behaviors (see Armitage & Conner, 2001).

The TPB has been applied in the context of online behavior, including adolescents' unfriending behavior on Facebook (Verswijvel et al., 2019) and acceptance of requests from strangers on social networking sites (Heirman et al., 2016), and there is support for the relationships specified in the model. Saeri et al. (2014) used the TPB to predict Facebook users' online privacy protection intentions and behaviors in a sample of 119 university students. However, only subjective norms predicted intentions to protect one's privacy online; neither intentions nor PBC predicted privacy protection behavior. There was, however, more support for some of the additional variables included in their extended TPB model. That is, descriptive norms (i.e., the perception that important others protected their privacy online) and perceived risk emerged as significant independent predictors of intentions. Ho et al. (2017) found more support for the original TPB model in a sample of 4920 13- to 19-year-olds: attitudes, subjective norms, and PBC all predicted privacy protection behaviors on social networking sites, although subjective norms emerged as the strongest predictor.

It should be noted that this previous research testing the TPB in the context of Facebook privacy protection was conducted prior to the privacy scandals. However, it is not unreasonable to expect that high profile scandals that call into question one's privacy on Facebook might alter the strength of the relationships between the elements of the TPB and intentions or require that additional predictors should be added to an extended model. For example, although trust did not emerge as a significant predictor in Saeri et al. (2014), it is feasible that trust – in other Facebook users or in Facebook itself – has become a more important predictor due to recent events. Moreover, previous research has not examined the role of privacy concerns within the TPB, even though privacy concerns are a major concern for internet users (e.g., Masur & Trepte, 2021; Quan-Haase & Ho, 2020; Sharma et al., 2018). Thus, it is worth revisiting the role of the TPB in predicting online privacy behaviors in relation to Facebook. The present research aims to replicate and extend previous research by testing the ability of an extended TPB model, which included additional normative factors as well as perceived risk, trust, and privacy concerns.

The role of injunctive and descriptive norms

In the original conceptualization of the TPB, norms refer to injunctive norms: perceptions of the level of approval for a behavior. However, it has been argued that norms consist of both injunctive and descriptive elements (Cialdini et al., 1990, 1991). Descriptive norms refer to perceptions of the level of engagement, or prevalence, of the behavior. It is now well accepted that descriptive norms play an important role in the TPB (e.g., Manning, 2009), and descriptive elements of norms are now incorporated routinely into the TPB (Ajzen, 2006). Within the context of online privacy behaviors, Saeri et al. (2014) found that both injunctive and descriptive norms were independent predictors of privacy protection intentions and suggested that a failure to distinguish between these types of norms may account for previous failures to find support for the role of norms (e.g., Yao & Linz, 2008). Given this, the present research incorporated both injunctive and descriptive norms to predict online privacy protection intentions and behavior.

The role of group norms

Another criticism of the way in which norms are conceptualized in the TPB comes from the social identity approach, which argues that the TPB focuses only on interpersonal dynamics and fails to account for the role of group processes (see Terry & Hogg, 1996). That is, within the TPB social pressure is seen to be additive across all referents (i.e., “most people who are important to me”). As such, the model fails to acknowledge that individuals differ in the extent to which they identify with referents and that certain sources of norms will be more important than others. From a social identity approach, the norms of salient social groups should influence intentions because the process of psychologically belonging to a group means that self-perceptions, attitudes, and behaviors are brought into line with the position specified by the group norm. Indeed, there is good support for the role of group norms in predicting intentions, even after accounting for interpersonal (or “subjective”) norms as conceived within the TPB (e.g., White et al., 2009; see; Hogg & Smith, 2007, for a review).

Saeri et al. (2014) noted that it might be important to consider the role of group norms as well as interpersonal norms to understand privacy protection behavior. That is, Facebook explicitly encourages the sharing of personal information, establishing a positive injunctive norm of disclosure among users. However, Saeri and colleagues did not assess injunctive and descriptive norms in relation to “other Facebook users”. In the present research, injunctive and descriptive norms were assessed at both the interpersonal level (i.e., “most people who are important to me”) and group level (i.e., “other Facebook users”) to assess the role of normative factors more fully in predicting online privacy protection intentions. In addition to broadening the normative component of the TPB, the present research also investigated the role of other variables found to be related to online privacy protection: risk, trust, and privacy concerns.

Risk, privacy concerns, and trust in online privacy protection

Risk perceptions

Risk perceptions are an important cue in social judgments (Jørgensen et al., 2013). Perceived risk is a subjective judgment that individuals feel about the features and seriousness of a risk and can serve as a warning of the potential negative consequences of an action (Youn & Hall, 2008). Risk perception has been studied widely in the context of online behavior (e.g., Acquisti et al., 2015; Adjerid et al., 2018; Gross et al., 2005).

People tend to disclose more private information when privacy risks are lower, such as when privacy policies are clearly understandable (Weber, 2009), while perceiving online activities as risky is associated with reduced service use (Lee, 2009) and with increased privacy protection (Paine et al., 2007). Saeri et al. (2014) noted that past work on risk and privacy protection conflated perceived risk with positive attitudes to privacy protection by conceptualizing risk as “privacy concerns.” In their research they focused on the role of implicit perceived risk within the TPB, finding that perceived risk was a unique predictor of online privacy protection intentions, but not behavior. In the present research, we investigated the roles of both risk perception and privacy concerns as predictors of online privacy protection intentions on Facebook.

Online privacy concern

There are many conceptualizations of privacy in online contexts (see Stuart et al., 2019, for a review). Online privacy refers to a user’s assessment of how accessible their information while they are interacting with other users and institutions, and whether they can shape this level of accessibility through self-disclosure and/or privacy regulation (Trepte, 2020). Privacy concern reflects the desire to keep personal information out of the hands of others and should be related to taking action to protect one’s privacy online. However, the relationship between privacy concerns and online privacy behavior is not straightforward (Hallam & Zanella, 2017). For example, while some research has found that privacy concerns have an impact on willingness to disclose personal information online (e.g., Aïmeur

& Sahnoune, 2020; Ampong et al., 2018; Li & Kobsa, 2020; Sun et al., 2019), other research has found that online privacy concerns are not a significant predictor of online self-disclosure behaviors (e.g., Oghazi et al., 2020; Zafeiropoulou, 2014). In the context of the TPB, Ho et al. (2017) found a significant, albeit small, positive relationship between privacy concerns and adolescents' intentions to protect their privacy. Online privacy concerns were included here as an additional predictor to further explore the effect of privacy concerns on online privacy protection intentions.

Trust

Trust is critical in understanding when an individual will choose to protect their privacy online and when they will choose to share personal information. Trust has been found to be an important construct in online contexts (Tang & Liu, 2015). Wu et al. (2012) found that trust has a significant positive impact on online self-disclosure, and some research has found that trust mediates the relationship between privacy concerns and willingness to disclose personal information online (Joinson et al., 2010; Olivero & Lunt, 2004). However, Saeri et al. (2014) did not find that trust was associated with online privacy protection intentions. The lack of support for the role of trust in Saeri et al. might reflect the way trust was measured. Specifically, the researchers assessed trust in "all Facebook users," a group that is very large and is likely to include highly trusted (e.g., friends) and untrusted (e.g., hackers) targets. Indeed, the mean level of trust reported was very low (1.9 on a 7-point scale). In the present research, we asked about trust in Facebook, rather than trust in other users. Trust in relation to Facebook is likely to be more important in understanding online privacy protection, given concerns about how Facebook uses and shares data (Brotman, 2019).

The present study

The aim of the present study is to understand online privacy protection behavior for Facebook users using an extended TPB model that broadens the normative component of the original model and also adds perceived risk, online privacy concerns, and trust to the original model (Figure 1). Our study draws upon the earlier work of Saeri et al. (2014) who found partial support for an extended TPB in this context and examines whether the original findings hold given recent innovations and scandals in relation to Facebook. However, we extend Saeri et al. in several ways. First, given new standards in

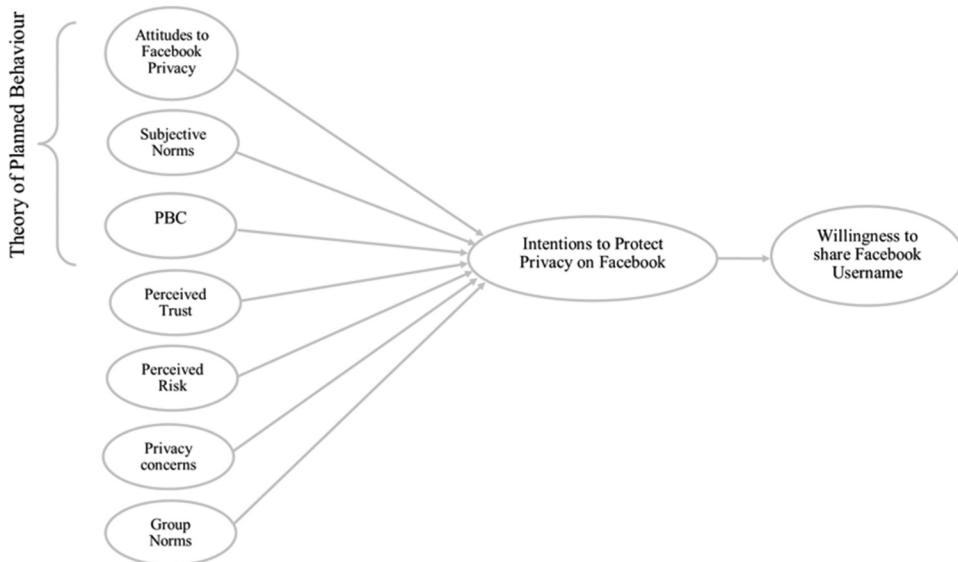


Figure 1. Extended theory of planned behavior Model.

relation to power and sample size, we sought to recruit a larger sample than the original study. Second, most research on online privacy in relation to Facebook has typically recruited from younger (i.e., student) samples; here, we recruited from a broader age range. Finally, we considered the role of group norms and online privacy concerns in predicting online privacy protection intentions.

In line with the TPB and Saeri et al. (2014), we predicted that positive attitudes to privacy protection, subjective norms in favor of privacy protection (injunctive and descriptive), and perceived behavioral control will be positively related to intentions to protect one's privacy on Facebook (H1). We further predicted that perceiving that other Facebook users approve of (group injunctive) and engage in (group descriptive) online privacy protection behaviors will be positively associated with online privacy protection intentions (H2). Further, we predict that higher levels of perceived risk (H3) and online privacy concerns (H4) would be positively related to intentions, while lower levels of trust in Facebook would be negatively related to intentions (H5). Finally, it is expected that intentions to protect privacy online will be associated with lower willingness to allow others to view one's Facebook profile (H6).

Method

Participants

Participants were 376 Facebook users (54% female¹) recruited via an undergraduate participant pool ($n = 94$), the crowdsourcing participant pool Prolific ($n = 264$), and social media ($n = 18$).² Undergraduate students received partial course credit and participants recruited via Prolific were paid £0.95 for their participation. The sample size was not based on a power analysis but reflects the number of participants able to be recruited within the time frame of the project and the funding available for participant reimbursement. Sensitivity analysis, using $\alpha = .05$ and .80 power, indicated that we had sufficient power to detect a small effect size of $f^2 = .04$. Participants' ages ranged from 18 to 65 years ($M_{\text{age}} = 29.89$; $SD = 9.69$). Ethical approval was obtained from the local ethics committee prior to data collection and all participants provided informed consent prior to participation.

Design

Key elements of the TPB such as attitudes, subjective injunctive norms, subjective descriptive norms, and perceived behavioral control served as independent predictors of privacy protection intentions and behavior. Furthermore, injunctive, and descriptive group norms, trust in Facebook, perceived risk, and privacy concerns were also our independent variables. Participants' online privacy protection intentions on Facebook and willingness to share Facebook username were our dependent variables.

Measures

The TPB variables were adapted from Ajzen (2006) and Saeri et al. (2014). Unless otherwise stated, all items were measured using seven-point scales (1 *strongly disagree*, 7 *strongly agree*).

Demographics

Participants reported their gender and age.

Attitudes to internet privacy and Facebook privacy

Participants' attitudes toward protecting their privacy online and toward protecting their privacy on Facebook were measured with five items (e.g., "When I personally think about protecting my privacy when using the internet in the future [using Facebook], I consider doing so to be:" bad-good). High scores indicated more positive attitudes toward online privacy protection ($\alpha = .83$) and protecting privacy on Facebook ($\alpha = .88$).³

Subjective injunctive norm

Four items assessed subjective injunctive norms (e.g., “The people in my life whose opinions I value would approve of me protecting my privacy on Facebook by controlling access to my personal information using the privacy settings in the future”). High scores indicated stronger perceived approval for Facebook privacy protection ($\alpha=.83$).⁴

Subjective descriptive norm

Subjective descriptive norms toward Facebook privacy protection were measured with four items (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 in the future themselves”). High scores indicated stronger perceived engagement in Facebook privacy protection ($\alpha=.84$).⁵

Perceived behavioral control

PBC was measured with four items (e.g., “I think I have control over protecting my privacy on Facebook by controlling access to my personal information using the privacy settings in the future”). High scores indicated stronger perceived behavioral control ($\alpha=.88$).⁶

Group injunctive norm

Injunctive group norms were measured with three items that asked about perceived approval for privacy protection among Facebook users (e.g., “In general, other Facebook users approve of online privacy protection”). One, reverse-scored, item was removed due to poor scale reliability (“In general, other Facebook users think that I should disclose personal information on my publicly accessible Facebook profile”) and the other two items were combined to form a scale, with higher scores indicating more positive injunctive group norms ($r(376)=.44$, $p < .001$).

Group descriptive norms

Descriptive group norms were measured with three items (e.g., “In general, other Facebook users do protect their privacy online”). One, reverse-scored, item was removed due to poor scale reliability (“In general, other Facebook users disclose personal information on their publicly accessible Facebook profile”); the remaining two items were averaged to form a scale with higher scores indicating more positive descriptive group norm ($r(376)=.71$, $p < .001$).

Trust

Participants’ trust toward Facebook was assessed with five items adapted from previous research (Chang et al., 2016; Doney et al., 1998; Gefen et al., 2003; Jang et al., 2015; Jin, 2013; e.g., “I think Facebook will keep its promises to users”). Higher scores indicated greater trust in Facebook ($\alpha=.85$).

Perceived risk

Four items, adapted from Chang et al. (2016) assessed participants’ perceived risk (e.g., “Using Facebook might involve some unexpected problems.”). One item was removed due to poor reliability (“I’m aware of the risks associated with using Facebook”); the remaining items were averaged to form a scale with higher scores demonstrating greater perceived risk ($\alpha = .617$).

Privacy concern

Participants’ privacy concerns were measured with four items adapted from previous research (Chang et al., 2015, 2016; Lankton & McKnight, 2011; e.g., “I am concerned about submitting information on the Internet, because of what others might do with it.”). Higher scores indicated greater privacy concerns ($\alpha=.88$).

Intentions

Participants' intentions to protect their privacy on Facebook were assessed with three items (e.g., "I plan to protect my privacy on Facebook by controlling access to my personal information using the privacy settings in the future"). Higher scores indicated greater intentions to protect one's privacy on Facebook ($\alpha=.95$).

Willingness to share Facebook username

Participants were asked to complete the checklist used by Saeri et al. (2014) to assess online privacy protection. The checklist represents a series of personal information categories (birthday, relationship status, home address etc.) on Facebook profiles, where users can indicate the visibility settings for each item. After completing the checklist, participants were asked to give their consent to the researchers to check the accuracy of their responses. Whether consent was given or not (1=consent given, 0=consent not given) was analyzed as an additional quasi-behavioral measure; however, participants were not actually asked for their profile details.

Procedure

Participants started the study by reading an information sheet that advised them that their participation was voluntary, that any identifying information would not be kept, and that they were free to withdraw at any time. The participant was provided with a general description of the study, a declaration of ethical clearance and contact details for the researcher. After providing informed consent, participants completed an online questionnaire assessing their attitudes, subjective norms (injunctive and descriptive), perceived behavioral control, group norms (injunctive and descriptive), privacy concerns, perceived risk, trust in Facebook, and intentions toward protecting their privacy online. On completion, participants completed a checklist to indicate what information is currently visible on their Facebook profile. After completing the checklist, participants were asked to provide consent for the researchers to look at their Facebook profile. At the end of the study, participants were debriefed on the deception involved and the purpose of the research. All measures are available at (<https://doi.org/10.17605/OSF.IO/QAZVU>).

Results

Descriptive statistics

The means, standard deviations, and bivariate correlations for all variables are presented in Table 1.

Overview of regression analyses

To predict intentions, a hierarchical multiple regression analysis was conducted (see Table 2). The TPB variables (attitudes to internet privacy and privacy on Facebook, subjective injunctive norm, subjective descriptive norm, and perceived behavioral control) were entered at Step 1,⁸ while the additional predictors (i.e., injunctive group norm, descriptive group norm, trust, perceived risk, and privacy concern) were entered at Step 2. To predict behavior, a logistic regression analysis was conducted (see Table 3), in which intentions were added at the final step.⁹

Online privacy protection intentions and behavior

Intentions

At Step 1, the TPB variables explained 36% of the variance in intentions, $R^2_{ch}=.357$, $F(5, 368) = 40.91$, $p<.001$. Inspection of the beta coefficients revealed that attitudes to Facebook privacy ($\beta=.178$, $p=.002$), PBC ($\beta=.160$, $p < .001$), injunctive norms ($\beta=.251$, $p < .001$), and descriptive norms ($\beta=.211$, $p < .001$)

Table 1. Means, standard deviations and inter correlations among the variables.

Variable	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Age	29.89	9.69	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. Gender	1.57	0.50	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. Attitudes to internet privacy	5.89	0.97	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. Attitudes to Facebook privacy	5.92	1.06	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. Subjective injunctive norms	5.56	0.98	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. Subjective descriptive norms	5.36	0.97	–	–	–	–	–	–	–	–	–	–	–	–	–	–
7. Perceived Behavioral Control	4.98	1.26	–	–	–	–	–	–	–	–	–	–	–	–	–	–
8. Group injunctive norms	5.10	1.09	–	–	–	–	–	–	–	–	–	–	–	–	–	–
9. Group descriptive norms	4.12	1.36	–	–	–	–	–	–	–	–	–	–	–	–	–	–
10. Trust	4.03	1.18	–	–	–	–	–	–	–	–	–	–	–	–	–	–
11. Perceived Risk	4.36	1.08	–	–	–	–	–	–	–	–	–	–	–	–	–	–
12. Privacy Concerns	5.60	1.05	–	–	–	–	–	–	–	–	–	–	–	–	–	–
13. Intentions	5.94	0.90	–	–	–	–	–	–	–	–	–	–	–	–	–	–
14. Willingness to share username	1.50	0.50	–	–	–	–	–	–	–	–	–	–	–	–	–	–

* $p < .05$, ** $p < .01$; gender coded as 1=Male, 2=Female, 3=Prefer not to say.

Table 2. Hierarchical multiple regression analysis of intentions to protect privacy on Facebook: block (R^2 ch) and coefficients (β), and 95% confidence intervals for B.

Predictor	Block 1		Block 2	
	β	95% Cis	β	95% Cis
Attitudes to internet privacy	.02	-.084, .114	-.06	-.151, .038
Attitudes to Facebook privacy	.18*	.055, .248	.18*	.059, .242
Subjective injunctive norms	.25**	.132, .329	.20**	.083, .275
Subjective descriptive norms	.21**	.098, .293	.21**	.101, .287
Perceived Behavioral control	.16**	.051, .177	.26**	.119, .252
Group injunctive norms			.04	-.048, .111
Group descriptive norms			-.15*	-.156, -.037
Trust			-.07	-.123, .022
Perceived risk			.01	-.062, .085
Privacy concerns			.27*	.153, .311
R^2 ch	.36**		.10**	
R^2	.36**		.46**	

* $p < .05$, ** $p < .01$.

Table 3. Logistic regression analysis of theory of planned behavior variables, trust, risk, privacy concerns, and intentions on consent to examine users' Facebook profiles (1 consent given, 0 consent not given): coefficients (B), odds ratio and pseudo r^2 .

Predictor	Model 1		Model 2		Model 3	
	B	Exp(B)	B	Exp(B)	B	Exp(B)
Attitudes to internet privacy	-.337*	1.164	-.281*	.755	-.278*	.757
Attitudes to Facebook privacy	.152	.714	.125	1.134	.119	1.126
Subjective injunctive norms	.030	1.030	.040	1.040	.033	1.033
Subjective descriptive norms	.210	1.233	.250	1.285	.243	1.275
Perceived Behavioral control	.096	1.10	-.025	.975	-.032	.968
Group injunctive norms	-		.100	1.105	.098	1.103
Group descriptive norms	-		-.073	.929	-.070	.932
Trust	-		.201	1.222	.203	1.225
Perceived risk	-		-.002	.998	-.002	.998
Privacy concerns	-		-.166	.847	-.175	.840
Intentions	-		-		.038	1.039
X^2 Block	10.827 ⁺		8.190		.054	
X^2 Model	10.827 ⁺		19.017*		19.071 ⁺	
Nagelkerke pseudo r^2	.039		.068		.069	

+ $p < .06$, * $p < .05$, ** $p < .01$.

were significant predictors of intentions to protect privacy on Facebook. That is, the more positive participants' attitudes to Facebook privacy, the more they perceived control over their Facebook privacy behaviors, the more participants perceived that important others approved of online privacy protection, and that important others engaged in online privacy protection themselves, the stronger their intentions toward online privacy protection.

The inclusion of injunctive group norms, descriptive group norms, trust, perceived risk, and privacy concerns at Step 2 accounted for an additional 10% of the variance in intentions, $R^2_{ch} = .10$, $F(5, 363) = 13.34$, $p < .001$. Inspection of the beta weights revealed significant effects only for descriptive group norms ($\beta = -.146$, $p = .002$) and privacy concerns ($\beta = .271$, $p < .001$). That is, participants reported *weaker* intentions to protect their privacy on Facebook when they perceived that other Facebook users were protecting their privacy. However, stronger privacy concerns were associated with stronger privacy protection intentions. In the final model, the variables accounted for 46% of the variance in online privacy protection intentions, $F(10, 363) = 30.56$, $p < .001$.

Willingness to share Facebook username

The TPB variables entered in the first block accounted for only a marginally significant proportion of the variance in privacy-protecting behavior, Omnibus test: $\chi^2(5, N = 361) = 10.827$, $p = 0.055$.¹⁰ Inspection of the coefficients revealed a significant effect for attitudes to internet privacy behavior

only, $B = -.337$, $p = .039$, $OR = .741$, such that participants who had more positive attitudes to internet privacy were less likely to agree to allow access to their Facebook profile. The entry of group-level injunctive and descriptive norms, privacy concerns, perceived trust, and risk in the second block did not explain additional variance in behavior, Omnibus test: $\chi^2(5, N = 361) = 8.190$, $p = .146$. Finally, the inclusion of intentions at the final step did not explain additional variance in behavior Omnibus test: $\chi^2(1, N = 361) = .054$, $p = .816$.

Discussion

The aim of the present research was to analyze online privacy protection in Facebook users using an extended TPB model that comprised injunctive and descriptive group norms, perceived risk, privacy concern, and trust. Overall, there was good support for the predictors specified in the TPB (H1): attitudes, subjective injunctive norms, subjective descriptive norms, and PBC all predicted intentions to engage in online privacy protection. There was mixed support, however, for the additional variables included in the extended TPB. Group descriptive norms, but not group injunctive norms, predicted online privacy protection intentions; however, the direction of this effect was opposite to predictions (H2). Online privacy concerns (H4), but not perceived risk (H3) or trust in Facebook (H5), also predicted intentions. Finally, online privacy protection intentions were not associated with behavior (i.e., willingness to share Facebook username; H6).

Theory of planned behavior

We predicted that Facebook users' attitudes toward privacy protection would predict their intentions to protect their privacy online. We found that specific attitudes toward privacy protection on Facebook, but not general attitudes to internet privacy, predicted Facebook privacy intentions. This finding is in line with the *principle of compatibility* (Fishbein & Ajzen, 1975). That is, attitudes that match the behavior in terms of specificity (i.e., attitudes to protecting privacy on Facebook) will be better predictors of behavioral intentions (i.e., privacy protection on Facebook) than more general attitudes (i.e., attitudes to protecting privacy on the internet). The finding that attitudes predict intentions is in line with the TPB and with other research in this specific domain (e.g., Yao & Linz, 2008; cf.; Saeri et al., 2014). In line with predictions and the work of Saeri et al. (2014), we found that both injunctive and descriptive norms were unique predictors of intentions, supporting the distinction between these sources of normative influence within the TPB. When participants believe that significant others approve of their online privacy protection and/or believe that others are likely to protect their own privacy, greater online privacy protection intentions are reported. Finally, and in line with the TPB, PBC emerged as a significant predictor of Facebook privacy protection intentions.

Overall, then, there was good support for the ability of the original TPB predictors to predict intentions to protect one's privacy on Facebook. This was in line with predictions, but somewhat inconsistent with Saeri et al. (2014), who only found support for the role of the normative component of the TPB. However, it should be noted that previous research applying the TPB in the domain of online behavior has often not found evidence for the role of *all* variables (e.g., Darvell et al., 2011; Lee, 2009; Yao & Linz, 2008; Yousafzai et al., 2010). It is likely that the increased power in our study and our sample had a more mixed-age profile compared to Saeri et al. (2014), accounts for the inconsistency in findings.

Our study found strong support for the TPB in predicting intentions; however, intentions were not associated with our quasi-behavioral measure (i.e., willingness to share Facebook username). Although this is consistent with Saeri et al. (2014), it is inconsistent with TPB predictions and other research applying the TPB to online behavior (e.g., Heirman & Walrave, 2012; Verswijvel et al., 2019; Yao & Linz, 2008). Given this, it is likely that the lack of association in the current research reflects the measurement of behavior. In the present analysis, we did not actually examine participants' Facebook profiles (cf. Saeri et al., 2014), but simply asked for consent to do so. It is possible that participants did not believe that we would look at their profiles, so that a different measure of behavior would reveal the

expected associations. Alternatively, our operationalization of privacy protection as participants' refusal of *experimenter* access to their profiles may have failed to align with participants' expectations of privacy threat sources (i.e., sinister cyber-criminals). Put differently, participants' trust in the experimenters specifically may have led participants to interpret providing their consent as a pro-social act benefitting the science of privacy, rather than interpreting the decision as facing a privacy threat per se (see e.g., Haslam et al., 2014). Nevertheless, it is interesting to note that only 50% of our participants were willing to give consent, compared to 96% of the participants in Saeri et al. (2014). In addition, attitudes to privacy protection did predict refusal of experimenter access in the present results. Future research should consider other ways to assess actual behavior to better understand the relationship between intentions and behavior in this context.

Injunctive and descriptive group norms

In addition to testing the role of injunctive and descriptive norms at the interpersonal (or “subjective”) level, we also looked at the role of group norms (i.e., other Facebook users). Results revealed that group descriptive norms, but not group injunctive norms, predicted Facebook privacy protection intentions. However, the direction of the effect was inconsistent with expectations: the more participants perceived that other Facebook users were engaging in privacy protection, the lower their intentions to protect their own privacy on Facebook. This finding, however, was only observed when other variables were controlled; at the zero-order level, group descriptive norms were not associated with intentions, a finding that is also inconsistent with most research looking at the role of group norms in the TPB. In general, descriptive group norms should have a positive association with intentions (see e.g., Smith & Louis, 2009).

One explanation for this unexpected finding is that there is a “free rider” effect in this context (see e.g., Lev-Aretz & Strandburg, 2020). That is, when other variables such as general privacy concerns, trust in other users, and the privacy-protecting behaviors of one's friends are controlled, if individuals perceive that other Facebook users are protecting their privacy on the site, then they might feel less need to protect their individual privacy as they are protected by the actions of others. Another explanation might be that if people perceive others around them (particularly known others that they share with) do not protect their privacy, then they may sense that they need to do more as an individual to protect their own privacy. Another consideration is that we did not measure the level of identification with the group (i.e., “Facebook users”): previous research has found that conformity to group norms is greater for high identifiers than low identifiers (see e.g., Hogg & Smith, 2007). Thus, our sample might have included many “low identifiers”, with the result that participants were not motivated to comply with group norms. However, given that the zero-order associations were not significantly negative between group descriptive norms and intentions, the overall sample appears to have been more neutral than norm-rejecting. The present untheorized suppression effect for group descriptive norms should thus be replicated before being interpreted substantively, but the results do highlight two distinctive patterns for injunctive and descriptive norms, and the importance of distinguishing the two variables at both the interpersonal and group levels (see Smith & Louis, 2008).

Finally, group injunctive norm was not a unique predictor of behavioral intentions in the final model. This is perhaps not surprising, given the non-significant zero-order correlation and (as noted earlier) failure to consider the moderating role of identification. Nevertheless, despite our unexpected findings, the present research points to the potential role of *group* norms, as well as more interpersonal norms, in understanding online privacy protection intentions, which is likely to be a fruitful avenue for future research.

Roles of perceived risk, privacy concern, and trust

We also investigated the role of three variables previously established as important in understanding online behavior: perceived risk, privacy concern, and trust. Results revealed that online privacy concerns (H4), but not perceived risk (H3) or trust in Facebook (H5) predicted intentions.

Both online privacy concerns and perceived risk were included in recognition that, although related and often conflated in research (see Saeri et al., 2014), these constructs are not interchangeable. Although both privacy concerns and perceived risk were correlated with intentions at the bivariate level, only online privacy concerns emerged as a unique predictor of Facebook privacy protection intentions. The finding that privacy concerns predict intentions is consistent with previous research in this field (e.g., Aïmeur & Sahnoune, 2020; Joinson et al., 2010; Wu et al., 2012; cf.; Yao & Linz, 2008). However, the lack of support for the role of perceived risk is inconsistent with the work of Saeri and colleagues, who found that perceived risk predicted intentions, and might be considered surprising considering controversies surrounding the misuse of Facebook data, for example by Cambridge Analytica.

Previous research has found that perceived trust influences online self-disclosure (e.g., Frye & Dornisch, 2010; Taddei & Contena, 2013), and so we expected that participants who perceived low levels of trust in Facebook would report higher privacy protection intentions. However, we did not find evidence of a relationship between trust and privacy protection intentions. The lack of support for the role of trust might indicate that trust is not an important factor in privacy protection intention on social networking or social media sites (cf. e-commerce sites; e.g., Gefen et al., 2003), given the widespread use of such sites and their use in maintaining social connections, or that actions taken by Facebook following events such as the Cambridge Analytica scandal (e.g., apologies) communicate that the organization is trustworthy or is rebuilding trust (see Ayaburi & Treku, 2020; Stamato, 2008). It is also possible that trust mediates the relationship between other variables, such as privacy concerns or perceived risk, and online behavior (e.g., Joinson et al., 2010).

Finally, it should be noted that none of these additional variables were associated with individuals' willingness to share their Facebook usernames (see also Saeri et al., 2014). This is perhaps not surprising, given the limitations associated with this measure in the current study. However, we would note that it is not uncommon to find a disconnect between people's attitudes and beliefs about online activity and their actual behavior (i.e., the privacy paradox; see Acquisti et al., 2012; Brandimarte et al., 2013). Nevertheless, we did find that general attitudes to protecting oneself online were associated with our measure: participants with more positive attitudes to online privacy were less likely to consent to the research team viewing their Facebook profiles.

Applied implications

Our research has several implications for online privacy protection. First, given that attitudes, norms, PBC, and privacy concerns influenced privacy protection intentions, it is important that campaigns to increase privacy protection should specifically target these psychological factors. For example, education campaigns could target PBC by showing people how to protect their privacy online (e.g., by changing privacy settings on online profiles). In the present data, it is also clear that norms – assessed at both the interpersonal and group level – play a role in online privacy protection intentions. Moreover, our results show that it is important to consider the distinction between injunctive and descriptive norms and frame communications promoting online privacy protection accordingly.

Limitations and future directions

Some limitations of this study should be acknowledged. First, this study investigates online privacy protection intentions and behavior only in the context of Facebook. Thus, results may not be generalized to other online social networks. There are some studies found that willingness to self-disclosure in relation to privacy concerns and trust differ between social network services (e.g., Dwyer et al., 2007; Fogel & Nehmad, 2009). Future research could investigate privacy protection intentions and behaviors in other online social networks. Second, the data is based on self-report, which relies on individuals being able to accurately report subjective information. Cross-sectional data also does not allow for confidence in reporting causality. Thus, the findings need to be tested longitudinally and experimentally to demonstrate the direction of effects, and to see whether developing an intention to

increase one's privacy protection online is associated with changes in behavior over time. Third, the removal of the reverse scored item in the descriptive norm scale due to poor scale reliability may be indicative of the ambiguity surrounding the concept of privacy in everyday understanding, which can result in seemingly contradictory behavior. Depending on the context and the type of information being shared, individuals may hold the belief that both privacy protection and the sharing of personal information online coexist. Finally, the unexpected direction of the relationship between intentions and group descriptive norms presents an important aspect of our findings. It raises the question of whether perceived privacy plays a role in influencing individuals' willingness to disclose personal information within a group setting. The perception of privacy within a group may enable intimacy, as individuals who perceive space to be private are more likely to reveal more about themselves. This observation offers an avenue for future research, where an extension of the current study could explore the underlying motives for disclosure. Such research would contribute to the existing literature by shedding light on the complex interplay between privacy and intimacy.

Conclusion

In this study, we analyzed online privacy protection intentions on Facebook using an extended theory of the planned behavior model, providing an update and extension to the earlier work of Saeri et al. (2014) on this topic. Overall, we found good support for the predictive ability of the TPB in this context, as well as support for a broader conceptualization of social norms and the role of privacy concerns. Overall, the present research contributes to an understanding of individuals' privacy protection intentions. In an era where we are all increasingly online, and online privacy is increasingly under threat, further research should continue to investigate what drives privacy protection online and consider how insights from such work can be applied to develop effective interventions.

Notes

1. Due to experimenter error, the respondents recruited via social media did not complete the age and gender questions.
2. One-way ANOVAs tested for differences between the groups in terms of the predictors and criterion. See Supplementary Materials for more details.
3. *Scale reliability* for participants' attitudes toward protecting their privacy on Facebook in Saeri et al. (2014) study: $\alpha = .82$.
4. *Scale reliability* for subjective injunctive norms in Saeri et al. (2014) study: $\alpha = .65$.
5. *Scale reliability* for subjective descriptive norms in Saeri et al. (2014) study: $\alpha = .69$.
6. *Scale reliability* for PBC in Saeri et al. (2014) study: $\alpha = .63$.
7. *Scale reliability* for perceived risk in Chang et al. (2016): $\alpha = .85$.
8. As noted in Footnote 1, 18 respondents did not complete the age and gender questions. A hierarchical regression analysis in which age and gender were entered at Step 1 indicated that these variables did not account for a significant proportion of the variance in intentions, $R^2_{ch} = .002$, $F(2, 353) = .290$, $p = .749$, and inclusion of these variables did not change the substantive pattern of results. See Supplementary Material for more details.
9. Preliminary analyses suggested that there were differences in several of the predictors as a function of participant source. A hierarchical regression analysis in which two dummy codes representing source were entered at Step 1 indicated that neither dummy code was a significant predictor of intentions $R^2_{ch} = .000$, $F(2, 371) = .011$, $p = .989$, and inclusion of these variables did not change the substantive pattern of results. See Supplementary Material for more details.
10. As before, an analysis in which age and gender were entered at Step 1 indicated that these variables did not account for a significant proportion of the variance in behavior, $\chi^2(2, N = 345) = 2.470$, $p = .291$. Inclusion of age and gender at Step 1 did not change the substantive pattern of results, although the effects of attitudes to internet privacy were stronger if these variables are included.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The author(s) reported there is no funding associated with the work featured in this article.

Notes on contributors

Mustafa Biber is pursuing a PhD in Psychology at the University of Exeter. His research explores the significance of social identities in people's lives and examines how these identities affect interactions between humans and artificial intelligence (AI).

Winnifred R. Louis, PhD, is a Professor in the School of Psychology at the University of Queensland, Australia. With a focus on group behaviour, social influence, and identity, her research delves into radicalization, conflict resolution, and activism.

Joanne R. Smith, PhD, is a Professor at the University of Exeter, UK, with a specialization in social psychology. Her educational background is from the University of Queensland, focusing her research on the influence of group norms and social identity in various contexts such as political, environmental, and health-related behaviours.

Data availability statement

The research was pre-registered prior to data collection and the data and materials are available at <https://doi.org/10.17605/OSF.IO/QAZVU>

Open Scholarship



This article has earned the Center for Open Science badges for Open Data, Open Materials and Preregistered. The data and materials are openly accessible at <https://doi.org/10.1080/17439760.2023.2239781>

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2), 160–174. <https://doi.org/10.1509/jmr.09.0215>
- Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, 42(2), 465–488. <https://doi.org/10.25300/MISQ/2018/14316>
- Aïmeur, E., & Sahnoune, Z. (2020). Privacy, trust, and manipulation in online relationships. *Journal of Technology in Human Services*, 38(2), 159–183. <https://doi.org/10.1080/15228835.2019.1610140>
- Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Ajzen, I. (2006). *Constructing a TPB Questionnaire: Conceptual & Methodological Considerations*. <http://People.Umass.Edu/Aizen/Tpb.Html>.
- Ampong, G. O. A., Mensah, A., Adu, A. S. Y., Addae, J. A., Omoregie, O. K., & Ofori, K. S. (2018). Examining self-disclosure on social networking sites: A flow theory and privacy perspective. *Behavioral Sciences*, 8(6), 1–17. <https://doi.org/10.3390/bs8060058>
- Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology*, 40(4), 471–499. <https://doi.org/10.1348/014466601164939>
- Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, 50(1), 171–181. <https://doi.org/10.1016/j.ijinfomgt.2019.05.014>
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 4(3), 340–347. <https://doi.org/10.1177/1948550612455931>
- Brotman, S. N. (2019, December 8). *Digital Trust is Essential for Data Privacy Protection*. Retrieved February 16, 2022, from <https://jia.sipa.columbia.edu/online-articles/digital-trust-essential-data-privacy-protection>

- Brown, A. J. (2020). "Should I stay or should I leave?": Exploring (Dis)continued Facebook use after the Cambridge analytica scandal. *Social Media & Society*, 6(1), 205630512091388. <https://doi.org/10.1177/2056305120913884>
- Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, 115(1), 88e106. <https://doi.org/10.1108/IMDS-07-2014-0197>
- Chang, S. E., Liu, A. Y., & Shen, W. C. (2016). User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behaviour*, 69, 207–211. <https://doi.org/10.1016/j.chb.2016.12.013>
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51. <https://doi.org/10.1016/j.chb.2017.12.001>
- 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 behaviour. *Advances in Experimental Social Psychology*, 24, 201–233. [https://doi.org/10.1016/S0065-2601\(08\)60330-5](https://doi.org/10.1016/S0065-2601(08)60330-5)
- 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(6), 1015–1026. <https://doi.org/10.1037//0022-3514.58.6.1015>
- 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. <https://doi.org/10.1089/cyber.2011.0035>
- Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review*, 23(3), 601–620. <https://doi.org/10.5465/AMR.1998.926629>
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Association for Information Systems - 13th Americas Conference on Information Systems, AMCIS 2007: Reaching New Heights*, Keystone, Colorado.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley.
- Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behaviour*. Psychology Press. <https://doi.org/10.4324/9780203838020>
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160. <https://doi.org/10.1016/j.chb.2008.08.006>
- Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior*, 26(5), 1120–1127. <https://doi.org/10.1016/j.chb.2010.03.016>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly: Management Information Systems*, 27(1), 51–90. <https://doi.org/10.2307/30036519>
- Graham-Harrison, E., & Cadwalladr, C. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge analytica in major data breach. *The Guardian*.
- Gross, R., Acquisti, A., & Heinz, H. J. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society - WPES '05*. <https://doi.org/10.1145/1102199.1102214>
- Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, 68, 217–227. <https://doi.org/10.1016/j.chb.2016.11.033>
- Haslam, S. A., Reicher, S. D., & Birney, M. E. (2014). Nothing by mere authority: Evidence that in an experimental analogue of the Milgram paradigm participants are motivated not by orders but by appeals to science. *Journal of Social Issues*, 70(3), 473–488. <https://doi.org/10.1111/josi.12072>
- Heirman, W., & Walrave, M. (2012). Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behaviour. *Psicothema*, 24(4), 614–620. <http://www.ncbi.nlm.nih.gov/pubmed/23079360>
- Heirman, W., Walrave, M., Vermeulen, A., Ponnet, K., Vandebosch, H., & Hardies, K. (2016). Applying the theory of planned behaviour to adolescents' acceptance of online friendship requests sent by strangers. *Telematics and Informatics*, 33(4), 1119–1129. <https://doi.org/10.1016/j.tele.2016.01.002>
- Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge analytica scandal. *International Journal of Human-Computer Studies*, 103, 102498. <https://doi.org/10.1016/j.ijhcs.2020.102498>
- Hogg, M. A., & Smith, J. R. (2007). Attitudes in social context: A social identity perspective. *European Review of Social Psychology*, 18(1), 89–131. <https://doi.org/10.1080/10463280701592070>
- Ho, S. S., Lwin, M. O., Yee, A. Z. H., & Lee, E. W. J. (2017). Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior and Social Networking*, 20(9), 572–579. <https://doi.org/10.1089/cyber.2017.0061>
- Internet World Stats. (2023). Internet usage statistics. <http://www.internetworldstats.com/stats.htm>
- Jang, Y.-T., Chang, S. E., & Chen, P.-A. (2015). Exploring social networking sites for facilitating multichannel retailing. *Multimedia Tools and Applications*, 74(1), 159–178. <https://doi.org/10.1007/s11042-013-1430-z>
- Jin, C. H. (2013). The perspective of a revised TRAM on social capital building: The case of Facebook usage. *Information & Management*, 50(4), 162–168. <https://doi.org/10.1016/j.im.2013.03.002>

- Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1), 1–24. <https://doi.org/10.1080/07370020903586662>
- Jørgensen, Ø., Bäckström, M., & Björklund, F. (2013). Bidirectional correction in social judgments: How a cue to the risk of bias causes more favourable ratings of some groups but less favourable of others. *Journal of Social Psychology*, 153(2), 131–148. <https://doi.org/10.1080/00224545.2012.711382>
- Lankton, N. K., & McKnight, D. H. (2011). What does it mean to trust Facebook? Examining technology and interpersonal trust beliefs. *The Data Base for Advances in Information Systems*, 42(2), 32–54. <https://doi.org/10.1145/1989098.1989101>
- Lee, M. (2009). Predicting and explaining the adoption of online trading: An empirical study in Taiwan. *Decision Support Systems*, 47(2), 133–142. <https://doi.org/10.1016/j.dss.2009.02.003>
- Lev-Aretz, Y., & Strandburg, K. J. (2020). Privacy regulation and innovation policy. *Yale Journal of Law and Technology*, 22. https://go.gale.com/ps/i.do?id=GALE%7CA622369531&sid=googleScholar&v=2.1&it=r&linkaccess=fulltext&issn=&p=AONE&sw=w&userGroupName=loyoland_main
- Li, Y., & Kobsa, A. (2020). Context and privacy concerns in friend request decisions. *Journal of the Association for Information Science and Technology*, 71(6), 632–643. <https://doi.org/10.1002/asi.24291>
- Manning, M. (2009). The effects of subjective norms on behaviour in the theory of planned behaviour: A meta-analysis. *British Journal of Social Psychology*, 48(4), 649–705. <https://doi.org/10.1348/014466608X393136>
- Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research*, 47(1), 49–74. <https://doi.org/10.1093/hcr/hqaa012>
- Nabity-Grover, T., Cheung, C. M. K., & Thatcher, J. B. (2020). Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media. *International Journal of Information Management*, 55(June), 102188. <https://doi.org/10.1016/j.ijinfomgt.2020.102188>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100–126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N. P., & Rad, F. F. (2020). User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts. *Journal of Business Research*, 112, 531–540. <https://doi.org/10.1016/j.jbusres.2019.12.006>
- Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), 243–262. [https://doi.org/10.1016/S0167-4870\(02\)00172-1](https://doi.org/10.1016/S0167-4870(02)00172-1)
- 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(6), 526–536. <https://doi.org/10.1016/j.ijhcs.2006.12.001>
- Quan-Haase, A., & Ho, D. (2020). Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology*, 71(9), 1089–1102. <https://doi.org/10.1002/asi.24364>
- Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behaviour. *Journal of Social Psychology*, 154(4), 352–369. <https://doi.org/10.1080/00224545.2014.914881>
- Sharma, K., Gupta, S., Gupta, P., & Arora, P. (2018). Users' perception on social media privacy concern. *2018 4th International Conference on Computing Sciences (ICCS)*, 80–83. <https://doi.org/10.1109/ICCS.2018.00019>
- 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-behaviour relationship. *British Journal of Social Psychology*, 47(4), 647–666. <https://doi.org/10.1348/014466607X269748>
- Smith, J. R., & Louis, W. R. (2009). Group norms and the attitude-behaviour relationship. *Social and Personality Psychology Compass*, 3(1), 19–35. <https://doi.org/10.1111/j.1751-9004.2008.00161.x>
- Stamato, L. (2008). Should business leaders apologize? Why, when and how an apology matters. *Ivey Business Journal Online*, 72(4), 1–8.
- Statista Research Department. (2019). Online Activities Ranked by Usage Penetration in Great Britain (GB) 2019. <https://www.statista.com/statistics/289048/online-activities-ranked-by-usage-penetration-great-britain-uk/>
- Statista Research Department. (2023). Number of Facebook Users Worldwide 2008–2023. <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
- Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass*, 13(11). <https://doi.org/10.1111/spc3.12507>
- Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability*, 11(12), 3311. <https://doi.org/10.3390/su10023311>
- Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behaviour*, 29(3), 821–826. <https://doi.org/10.1016/j.chb.2012.11.022>
- Tang, J., & Liu, H. (2015). Trust in social media. Synthesis lectures on information security. *Privacy, and Trust*, 10(1), 1–129. <https://doi.org/10.2200/S00657ED1V01Y201507SPT013>

- Terry, D. J., & Hogg, M. A. (1996). Group norms and the attitude–behavior relationship: A role for group identification. *Personality and Social Psychology Bulletin*, 22(8), 776–793. <https://doi.org/10.1177/0146167296228002>
- Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, 31(4), 549–570. <https://doi.org/10.1093/ct/qtz035>
- Tuttle, H. (2018). Facebook scandal raises data privacy concerns. *Risk Management*, 65(5), 6–9. <https://uoelibrary.idm.oclc.org/login?url=https://search-proquest-com.uoelibrary.idm.oclc.org/docview/2101229017?accountid=10792>
- Verswijvel, K., Heirman, W., Walrave, M., & Hardies, K. (2019). Understanding adolescents' unfriending on Facebook by applying an extended theory of planned behaviour. *Behaviour and Information Technology*, 38(8), 807–819. <https://doi.org/10.1080/0144929X.2018.1557255>
- Weber, R. H. (2009). Internet of things – need for a new legal environment? *Computer Law & Security Review*, 25(6), 522–527. <https://doi.org/10.1016/j.clsr.2009.09.002>
- White, K. M., Smith, J. R., Terry, D. J., Greenslade, J. H., & McKimmie, B. M. (2009). Social influence in the theory of planned behaviour: The role of descriptive, injunctive, and in-group norms. *British Journal of Social Psychology*, 48(1), 135–158. <https://doi.org/10.1348/014466608x295207>
- Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behaviour*, 28(3), 889–897. <https://doi.org/10.1016/j.chb.2011.12.008>
- Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior*, 11(5), 615–617. <https://doi.org/10.1089/cpb.2007.0208>
- Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviours. *Cyberpsychology and Behaviour*, 11(6), 763–765. <https://doi.org/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(5), 1172–1202. <https://doi.org/10.1111/j.1559-1816.2010.00615.x>
- Zafeiropoulou, A. M. (2014). *A Paradox of Privacy: Unravelling the Reasoning Behind Online Location Sharing*. Unpublished doctoral thesis, University of Southampton. <https://eprints.soton.ac.uk/376477/>