Security and privacy in online social networking: risk perceptions and precautionary behaviour

Paul van Schaik[1,*], Jurjen Jansen[2], Joseph Onibokun[3], Jean Camp[4] and Petko Kusev[5]

To appear in Computers in Human Behavior

[1]Teesside University, School of Social Sciences, Business and Law, Middlesbrough, United Kingdom

[2]NHL University of Applied Sciences, Cybersafety Research Group, Leeuwarden, The Netherlands

[3]The Union Advertising Agency, Union Digital, Edinburgh, United Kingdom

[4]Indiana University, School of Computing, Bloomington, Indiana, United States of America

[5]University of Huddersfield, Huddersfield Business School, Department of Management, Huddersfield, United Kingdom

*Corresponding author

Security and privacy in online social networking: risk perceptions and precautionary behaviour

Abstract. A quantitative behavioural online study examined a set of hazards that correspond with security- and privacy settings of the major global online social network (Facebook). These settings concern access to a user's account and access to the user's shared information (both security) as well as regulation of the user's information-sharing and user's regulation of others' information-sharing in relation to the user (both privacy). We measured 201 non-student UK users' perceptions of risk and other risk dimensions, and precautionary behaviour. First, perceptions of risk and dread were highest and precautionary behaviour was most common for hazards related to users' regulation of information-sharing. Other hazards were perceived as less risky and less precaution was taken against these, even though they can lead to breaches of users' security or privacy. Second, consistent with existing theory, significant predictors of perceived risk were attitude towards sharing information on Facebook, dread, voluntariness, catastrophic potential and Internet experience; and significant predictors of precautionary behaviour were perceived risk, control, voluntariness and Internet experience. Methodological implications emphasise the need for non-aggregated analysis and practical implications emphasise interventions to promote safe online social-network use.

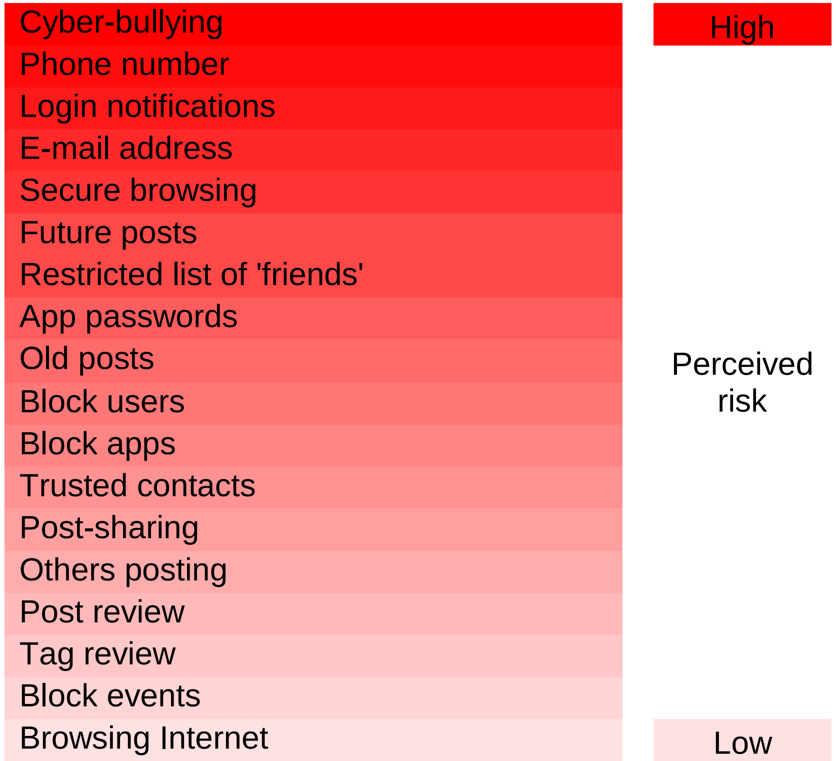
Keywords: online privacy; information security; social media; risk perception; Facebook; precautionary behaviour

Highlights

- We empirically studied users' response to security- and privacy settings in Facebook
- Perceived risk was highest for user's information-sharing related to privacy
- Use habits, attitude and risk dimensions predicted perceived risk
- Use habits, perceived risk and risk dimensions predicted precautionary behaviour
- This research has implications for data analysis and interventions

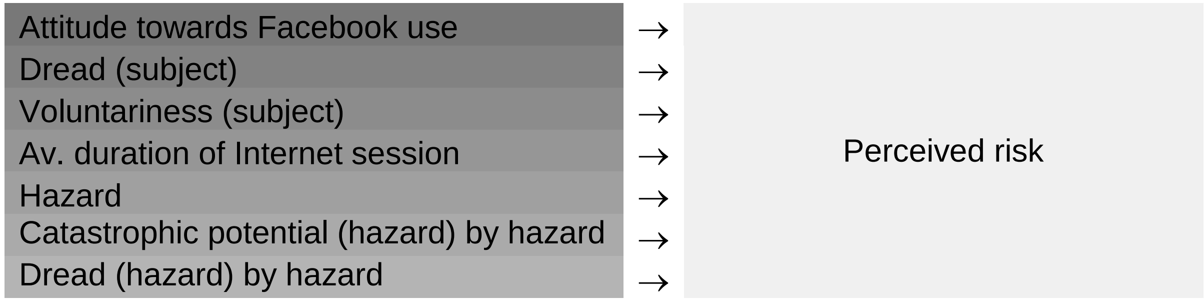
Security and privacy in online social networking: risk perceptions and precautionary behaviour

Risk variation among security hazards



Cyber-bullying
Phone number
Login notifications
E-mail address
Secure browsing
Future posts
Restricted list of 'friends'
App passwords
Old posts
Block users
Block apps
Trusted contacts
Post-sharing
Others posting
Post review
Tag review
Block events
Browsing Internet

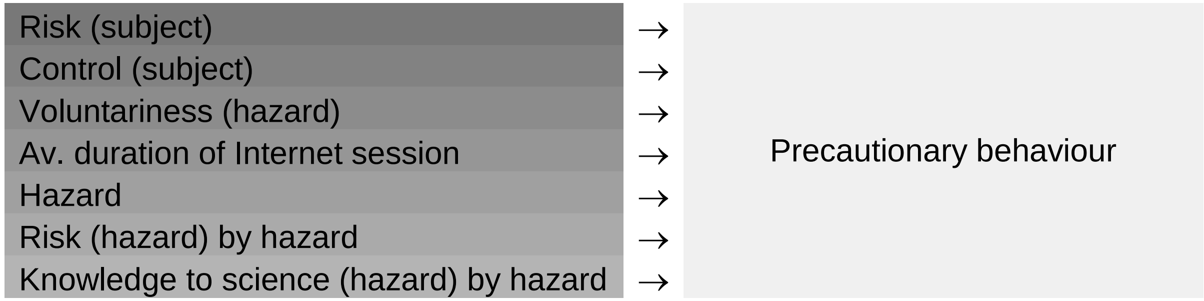
Hazard perception predicting perceived risk



Attitude towards Facebook use →
Dread (subject) →
Voluntariness (subject) →
Av. duration of Internet session →
Hazard →
Catastrophic potential (hazard) by hazard →
Dread (hazard) by hazard →

Perceived risk

Hazard perception predicting precautionary behaviour



Risk (subject) →
Control (subject) →
Voluntariness (hazard) →
Av. duration of Internet session →
Hazard →
Risk (hazard) by hazard →
Knowledge to science (hazard) by hazard →

Precautionary behaviour

Table of contents

1 Introduction

People are increasingly using online social networks (or social media[1]), such as Facebook, Twitter and LinkedIn. However, information-sharing by social-network users can result in violations of privacy (Garg & Camp, 2015) and security (Benson, Saridakis & Tennakoon, 2015). For example, a user whose contact details have been revealed may become the subject of harassment in a deliberate, repeated, and hostile manner (cyber-bullying) or become a potential victim of identity theft. It is therefore essential to study people's use of online social networks, especially where users are non-specialists in security and privacy, to reduce such violations (Garg & Camp, 2015). In particular, by developing models of human behaviour in relation to computer security and -privacy, research has aimed to develop a better understanding of this risk-related behaviour (Anderson & Agarwal, 2010; Liang & Xue, 2010). Risk perceptions continue to play a fundamental role in these models, both in security (Huang, Patrick Rau, Salvendy, Gao & Zhou, 2011) and privacy (Dinev, McConnell & Smith, 2015).

In the context of computer systems, three dimensions of information security (the protection of information by means of access control) are confidentiality (protection from unauthorised reading information), integrity (protection from unauthorised writing information) and availability (protection against actions that prevent reasonable access by legitimate users to their systems) (Schneier, 2015). Security is considered a necessary, but not sufficient requirement for privacy (Morton & Sasse, 2012). In this research, we study security- and privacy settings in Facebook.

Various conceptualisations of privacy have been published (e.g., Westin, 1967; Zureik & Stalker, 2010). In relation to online privacy, Dienlin and Trepte (2015) distinguish three types: informational privacy (control over the processing and transferring of personal information on line), social privacy (regulating proximity and distance toward others on line) and personal privacy (perceived control over emotional and cognitive outputs). The current study examines on the second type. We focus on privacy settings in social media because they play an important role in this regard by providing a mechanism for social privacy.

[1] The terms 'online social network' and 'social medium' are used interchangeably in the text.

The aim of this research is to study security- and privacy-related risk perceptions and precautionary behaviour in social-network use. Our goals are to (1) determine how different potential security- and privacy-related hazards in an online social network are perceived, (2) establish to the extent to which people take precautions against different potential security- and privacy-related hazards, and (3) ascertain the antecedents of risk perception and precautions taken against risk of security- and privacy violations.

2 Theoretical approaches to studying risk perception

Various approaches to studying risk perception have been published. For the present study, the most significant ones are the following. *Availability* ("the ease with which instances come to mind") influences people's risk perception (Kahneman, 2011, p. 129). Saliency (the extent to which an event attracts attention), dramatic nature of an event (e.g., a plane crash) and the source of experience (e.g., personal experiences) can enhance availability. According to the *affect heuristic*, the more technologies or activities are associated with positive feelings (e.g., sunbathing), the less they are judged to be risky and the more they are judged to be beneficial (Finucane, Alhakami, Slovic & Johnson, 2000).

Starr (1969) used population statistics of human behaviour to infer people's *revealed risk-related preferences* regarding particular technologies and human activities. He analysed the relationship between risk (the statistical expectation of death per hour of exposure) and benefit (the average amount of money spent per individual participant or the average contribution made to a participant's annual income) for some common activities. However, the approach of revealed preferences suffers from several shortcomings. First, preferences may not be stable over time and aggregate data do not take into account the variability among hazards (Fischhoff, Slovic, Lichtenstein, & Combs, 1978). Second, the underlying assumption that people both have full information and use that information optimally has been refuted (Simon, 1956). Third, different measures of risk and benefit lead to different conclusions (Fischhoff et al., 1978).

Psychometric methods have been used to study *expressed risk preferences* regarding particular technologies and human activities (Slovic, 1987). This has the advantage of eliciting perceptions (thoughts and judgments) of risk from people who are (potentially) exposed to particular risks that are studied, and can provide information about the causes of behaviour and potential ways to influence this. Applications of the results of work using these methods include risk communication (e.g., Young, Kuo & Chiang, 2014; Kim, Choi, Lee, Cho, & Ahn, 2015) and risk policy (e.g., Huang, Ban, Sun, Han, Yuan & Bi, 2013). From a set of risk dimensions (e.g., voluntariness, controllability and newness; see Online Appendix OA1), prediction equations of risk perception have been developed (Fischhoff et al., 1978). A limitation is that data are usually averaged over hazards. Therefore, the effect of or variability in hazards cannot be analysed, with (other) predictors held constant, and the analysis may not predict risk perceptions for individual hazards. Moreover, there is an apparent lack of research showing how risk perceptions 'translate' into behaviour. The current research combines the study of expressed preferences and revealed preferences. This enables us to pursue our goals: to quantify variation among hazards, and to predict risk perception and precautionary behaviour. Risk perceptions and precautionary behaviour have also been the subject of existing research on privacy and security of social media.

3 Privacy and security of social media

Privacy and security are major issues in social media. First, it has been noted that security and privacy design of social media is weak (Acquisti & Gross, 2006), thereby creating security- and privacy vulnerabilities. Second, the main purpose of social media, information-sharing, inherently has implications for privacy: for example, whom to share information with, what to share and how much to share. Given these issues, users' behaviour and underlying risk perceptions becomes even more important to protect against security- and privacy hazards.

Online security in social networks. Saridakis, Benson, Ezingeard and Tennakoon (2016) note an imbalance in behavioural research on online social networks, with many studies on privacy, but a dearth of research on security. They studied how social-network use and security perceptions are related to online victimisation. The results showed that with those with high perceived control over personal information on social networks, those with high perceived risk propensity on social networks and users of multi-purpose social networks are less likely to be cyber-crime victims, but users of knowledge exchange social networks are more likely to be victims.

Online privacy in social networks. Dienlin and Trepte (2015) distinguish informational, social and psychological privacy and study each of these privacy types empirically in Facebook. Based on the reasoned-action approach (Fishbein & Ajzen, 2011), privacy attitude, intention and behaviour were studied for each of the privacy types, but privacy concern was studied more generally, without reference to these types. The authors demonstrate that, for each of the three privacy types, privacy concerns were an indirect predictor of privacy behaviour, mediated by privacy attitude and privacy intention. Moreover, privacy attitude was an indirect predictor of privacy behaviour, mediated by privacy intention.

Taddicken (2014) studied willingness to self-disclose in social media rather than protecting existing information that a user has already entered as personal content rather than how people protect their information that they have already previously disclosed as personal content on an online social network. In disclosure, a distinction was made between sensitivity (facts versus sensitive) and access (open versus restricted). The findings show that privacy concerns are not a predictor of self-disclosure; perceived social relevance of online social networks are a predictor for self-disclosure of open facts and restricted sensitive information; and number of social networks used and general willingness to disclose are predictors of self-disclosure (except for self-disclosure of restricted facts).

Acquisti and Gross (2006) studied information-sharing by student-Facebook users. Various types of personal information were shared to a different extent (most users did not share cell-phone number, home-phone number, personal address, class schedule and partner's name; however, a majority did share birthday, political views and sexual orientation). There was little or no relation between participants' privacy attitudes and their information-sharing: students shared particular information, although the expressed concern about strangers identifying that information. As a potential explanation for this lack of correlation there was a lack of awareness in a significant minority regarding how to change their profile visibility in Facebook. Furthermore, a significant minority of users who had not changed the default privacy settings in Facebook incorrectly did not believe that any Facebook user can search their Facebook profile. Moreover, more than half of participants underestimated the number of people who could search their profile. Aware users claimed to be satisfied with their visibility and searchability on Facebook because although they were concerned about who could access their profiles, they claimed to manage these concerns by controlling the information they disclose.

Garg, Benton and Camp (2014) and Garg and Camp (2015) conducted a survey study using the psychometric paradigm to analyse university students' perception of risk to privacy by information-sharing on Facebook. In their analysis to predict perceived risk from (other) risk dimensions, knowledge by those exposed to privacy risk was a negative predictor; therefore, the more knowledgeable Facebook users, the less perceived risk. Arguably the most serious limitation of this work is that the data were collapsed over hazards in the regression analysis with perceived risk as the dependent variable and other risk dimensions as predictors. Moreover, perceived risk was measured as perceived benefit in half of the research participants.

Beldad (2016) found that risk perception and the perceived effectiveness of privacy settings were positive predictors of *precautionary privacy-related behaviour* (social privacy) through the use of Facebook privacy settings, but experience (years of Facebook use) was a negative predictor. Using a different outcome measure, Beldad (2015) found that positive predictors of *personal-information disclosure* (informational privacy) were benefits of information-sharing, experience and size of personal Facebook network. From these two studies, it follows that the predictors of precautionary behaviour and information disclosure differ or have a different sign (experience was negative predictor of precautionary behaviour, but a positive predictor of information disclosure).

Caine et al.'s (2011) showed that visualization of audience in an online social network can reduce personal-information disclosure relative to textual or numerical representation, thereby offering a potential tool for better aligning privacy preferences with privacy behaviour. Halevi et al. (2013) established that openness as a personality factor was positively correlated with the extent of posting information on Facebook and negatively correlated with strictness of Facebook privacy settings. Johnson et al. (2012) investigated Facebook users' privacy concerns. Users were most concerned about victimisation by thieves using Facebook as a means, employer seeing inappropriate content on their profile or assessing their suitability for the company from their profile and sexual predators using Facebook as a means.

Evaluation and rationale. Three main gaps are apparent in the literature. First, although risk perception is deemed an important predictor of precautionary behaviour in its own right (Huang et al., 2011; Keith, Thompson, Hale, Lowry & Greer, 2013) and is an important element of models of risk-related behaviour (Anderson & Agarwal, 2010; Liang & Xue, 2010), existing research has studied risk perception and risky behaviour in relation to online security or online privacy largely separately (e.g., Garg and Camp, 2015) or studied perception and behaviour in relation to each other without analysing specific hazards (Beldad, 2015; 2016; Shin, 2010). An exception is the work by Keith et al. (2013), but their analysis was confined to sharing location data and focused on disclosure of (mainly) new information (informational privacy) rather than a wider range of precautionary behaviours (social privacy) in an online social network. Another exception is Shin's (2010), who proposed and found evidence for perceived privacy as a predictor of perceived security. However, this work aimed to predict intention to use social media rather than to predict precautionary behaviour and did not study risk perception.

Second, in terms of specificity, either no specific behaviour (Beldad, 2015, 2016; Dienlin & Trepte, 2015) or only one specific behaviour (Joinson et al., 2010) was studied or several behaviours were measured but then analysed by aggregation (Garg & Camp, 2015). Therefore, variance between behaviours in risk perception and precautionary behaviour could not be established, although people's perceptions and behaviour may differ depending on the information item that is at stake (Kokolakis, 2017).

Third, several studies did not measure risk perception (Dienlin & Trepte, 2015; Taddicken, 2014; Acquisti & Gross, 2006; Cain et al., 2011; Halevi et al., 2013; Johnson et al., 2012). Thus, the role of risk perceptions in shaping specific behaviours (as predictors) could not be established.

The current study addresses these three gaps by studying both security and privacy in a social medium, studying specific behaviours and by studying both risk perception and precautionary behaviour in their own right and in relation to each other.

4 Current study

4.1 Variations in risk perception and precautionary behaviour

In online security and -privacy the actual risks are usually not known, so mechanisms such as availability or the affect heuristic may be even more influential than in other domains; for example, news reports can increase the availability of particular security- and privacy hazards and thereby increase the associated perceived risk, even though objectively the risk may not be increased. Therefore,

Research Question 1: how do users of an online social network perceive different potential security- and privacy-related hazards in terms of risk, benefit, and other risk dimensions? (cf., Fischhoff et al., 1978).

Moreover, as people may perceive certain social-network related hazards as riskier than others, they may (as a consequence) also act more cautiously in relation to some hazards than in relation to others (Keith et al., 2013). Thus,

Research Question 2: to what extent do users of an online social network take precautions against different potential security- and privacy-related hazards?

4.2 Predicting risk perception and precautionary behaviour

Extensive research has proposed various risk dimensions (see Online Appendix OA1) as predictors of perceived risk that are also relevant to the study of information security (Van Schaik, Onibokun, Coventry, Jansen & Kusev, 2017). From existing research and Van Schaik et al. (2017), Table 1 summarises the risk-related predictors of perceived risk.

Therefore,

Research Question 3: what are the antecedents of risk perception in users of an online social network?

According to existing models of human behaviour such as protection motivation theory, as perceived risk increases, people’s propensity to protect against this risk also increases (Floyd, Prentice-Dunn & Rogers, 2000). Therefore, the risk dimensions that predict perceived risk (discussed in relation to Research Question 3), are also potential predictors of precautionary behaviour (see Table 2). Previous research on risk perception supports this idea (Slovic, MacGregor & Kraus, 1987; Sjöberg, 2000) as well as the role of experience (Rosenboim, Benzion, Shahrabani & Shavit, 2012) and demographics (Layte, McGee, Rundle & Leigh, 2007) as predictors. Thus,

Research Question 4: what are the antecedents of precautions taken against risk in an online social network?

5 Method

5.1 Design

An online survey design was used. The within-subjects independent variable was hazard, with 16 levels (Table 3). Two further comparisons were also included: searching for information on line and cyber-bullying. For the purpose of this research, we define a hazard as a potential threat resulting from a particular privacy- or security setting in Facebook to a user's security or privacy, depending on the value that the user has chosen for this setting for their own Facebook account. We studied 16 hazards corresponding to Facebook security- and privacy-related settings, divided in four categories that were accessible as different sections through Facebook's user-interface at the time of the study (Table 3). Regarding security setting categories, account access corresponds with the security dimensions integrity and availability (Schneier, 2015), whereas information access corresponds to the security dimension confidentiality (Schneier, 2015). Regarding privacy setting categories, a user's regulation of information-sharing and a user's regulation of others' information-sharing in relation to the user can be considered as two specialisations of Dienlin and Trepte's (2015) privacy type 'social privacy': the first directed at self and the second directed at others.

The dependent variables were perceived risk, perceived benefit, risk balance (benefit minus risk; Bronfman & Cifuentes, 2003), and perceptions of eight further risk dimensions, and precautionary security- and privacy-related behaviour. Attitudes towards information-sharing on Facebook were also measured, and data on demographics and Internet use were collected.

5.2 Participants

Respondents were 201 Facebook users (109 male, 92 female; mean age = 42, *SD* = 17) from the UK, recruited through an online survey panel service (Maximiles UK Ltd). Consistent with the service's policy, they received an equivalent of £3 as a reimbursement. Of the sample, 55% had an education level of less than a first degree (bachelor's or undergraduate degree) and 58% was employed or self-employed. They were experienced Internet users (mean = 14 years, *SD* = 5) and used the Internet for various purposes besides social networking, most notably buying products or services (85%), using websites (84%) and reading news (77%). Most used the Internet daily (19% daily, 32% 2-3 times daily and 43% more than three times a day) and spent an hour or more on the Internet, once on line (25% about one hour, 42% several hours).

5.3 Measures

Sixteen items were 4 security settings for access to Facebook account; 4 security settings for access to shared information; 4 privacy settings/tools related to user's regulation of information-sharing; and 4 privacy settings related to user's regulation of others' sharing related to the user's Facebook content.[2]. These 16 items were selected because they were related to what were deemed to be Facebook's most clearly described security- and privacy settings at the time of data collection (April 2014). Two further comparison items were also included, at opposite ends of perceived risk (low: browsing Internet sites for information; high: cyber-bullying). These were not (directly) related to security and privacy of social media, but included as comparisons in addressing Research Question 1.

For each item, the following 10 dimensions of risk perception were measured, based on Fischhoff et al. (1978), and Bronfman, Cifuentes, Dekay and Willis (2007): perceived risk, benefit, voluntariness, immediacy of effect, knowledge about risk by affected population, knowledge about risk by science, control over risk, newness, (chronic-)catastrophic potential and dread (see Online Appendix OA1 for details). In

[2] The two types of privacy setting can be seen as two different mechanisms to achieve social privacy (Dienlin & Trepte, 2015), by regulating (1) access to one's personal online information and (2) other's behaviour in relation to access to one's personal online information.

response to each item (from the set of 16 hazards and 2 comparisons [Table 3]), participants had to give a rating on these 10 dimensions of risk perception, using a 7-point semantic-differential. For example, for the measurement of risk, participants had to rate the risk of each of the 18 items (e.g., sharing their telephone number) by way of a 7-point scale with endpoints ‘poses no risk’ (1) and ‘poses great risk’ (7).

Five standard items from social-cognition research were employed to measure attitudes towards sharing information on Facebook (Online Appendix OA1, Section 1.12; adapted from Davis, 1993); these used a 7-point semantic-differential response format, with a more positive attitude indicated by lower scores. Principal component analysis of the attitude items yielded a one-factor solution, explaining 77% of variance. Scale reliability was good – Cronbach’s alpha = 0.93. Therefore, an average attitude score was calculated and used in subsequent analysis.

Items measuring precautionary behaviour in terms of current use of security- and privacy-related settings (the 16 listed hazards) used a three-point scale (with responses ‘yes’, ‘no’, ‘don’t know’; Online Appendix OA1, Section 1.13). Each of these responses was later categorized as ‘safe’, ‘unsafe’ or ‘unknown’ (corresponding with an answer of ‘don’t know’) for each hazard. An answer was classified as safe or unsafe depending on whether the hazard was described as not taking a precaution or as taking a precaution (e.g., sharing phone number was classified as unsafe, but doing secure browsing was classified as safe).

5.4 Procedure

Questions on demographics were presented first (Online Appendix OA1, Section 1.1). Then for each of the 10 risk dimension questions, the meaning of the risk dimension was explained (Online Appendix OA1, Sections 1.2-1.11), and each of the 16 hazards and 2 comparison activities was presented per question. For each question, the 18 hazards/comparisons were presented consecutively (as a block) in random order. In turn, each block of questions was randomly presented. Next, the attitude questions were presented in random order (Online Appendix OA1, Section 1.12), followed by the questions on security- and privacy-related settings (Online Appendix OA1, Section 1.13), also in random order. On average, it took participants 33 minutes to complete the questionnaire.

6 Results

6.1 Analysis of hazards

In relation to *Research Question 1*, we analysed how Facebook users perceive different security- and privacy-related hazards. Confidence intervals of the mean (Table 4; Figure 1) indicate that perceived risk was highest for cyber-bullying, sharing telephone number, failing to (have made arrangements to) receive ‘login notifications’ and sharing e-mail address and lowest for browsing Internet sites for information. The converse was true for risk balance (Table 4). One-way analysis of variance (ANOVA) confirmed that the effect of hazard/comparison activity on risk perception, F (17, 3400) = 37.77, $\varepsilon^2 = .15$, $p < .001$, and risk balance, F (17, 3400) = 58.75, $\varepsilon^2 = .22$, $p < .001$, was significant. The effect of hazard was also significant when Internet-browsing and cyber-bullying were excluded from the analysis. Pairwise comparisons with Bonferroni correction for perceived risk showed that cyber-bullying was perceived as significantly riskier than all other hazards/activities, except sharing phone number. A similar pattern of results was found for risk balance and dread. Sharing phone number, sharing e-mail address, and failing to receive login notifications were perceived riskier than most remaining hazards/activities, but each of these did not differ significantly from the other two. Browsing the Internet for information was perceived to be less risky than all other hazards/activities.

Risk profiles were constructed per hazard/comparison, showing the mean for perceptions of risk, benefit, and eight other risk dimensions (Table 5). Hazards/activities seemed to differ most on perceived risk, perceived benefit, and dread. Analysis by risk dimension showed that the effect of hazard/comparison was significant for all perceived-risk dimensions, indicating significant variability among hazards/activities. The effect was strongest for perceived risk, benefit (both ε^2 = .15), and dread (ε^2 = .12). When Internet-browsing and cyber-bullying were excluded from the analysis, the effect was strongest on perceived risk and dread. Perceptions of dread showed the same pattern as perceived risk, with highest mean scores for cyber-bullying, sharing telephone number, sharing e-mail address, and failing to (have made arrangements to) receive ‘login notifications’, and lowest for browsing Internet sites for information.

As we studied risk perception of both security and privacy, we also compared risk perceptions of the different grouped types of security- and privacy-related hazards. Repeated-measures ANOVA (see also Figure 1) showed that the effect of hazard category (security/access to account, security/information access, privacy/information-sharing, and privacy/timeline and tagging) on perceived risk was significant, F (3, 600) = 43.73, $p < .001$, $\varepsilon^2 = .03$. Follow-up tests with Bonferroni correction showed that security hazards related to access to account were rated as riskier than security hazards related to information access, t (200) = 6.00, $p < .001$, d = 0.19. Privacy hazards related to regulation of information-sharing were perceived as riskier than privacy hazards related to regulation of others' information-sharing, t (200) = 9.17, $p < .001$, d = 0.33. Regulation of information-sharing was also riskier than access to account, t (200) = 3.34, $p < .01$, d = 0.10, and information access, t (200) = 8.53, $p < .001$, d = 0.23.

In relation to *Research Question 2*, we analysed to what extent users take precautions against security- and privacy-related hazards through their Facebook settings. Taking and failing to take precautions were analysed separately, as there were also participants who reported not knowing whether they had taken particular precautions. Over 50% of participants reported having taken precautions against potential violations of security and privacy through social-network settings for phone number (safe not to share), e-mail address (safe not to share), restricted list of 'friends' (safe to keep list) and blocking users (safe to block) (Table 6).

Moreover, the variables hazard (16 Facebook privacy- and security settings) and taking a precaution (yes/other) were not independent, Cramer's $V = .25$. Follow-up contrast analysis with Bonferroni correction showed that phone number (more precautionary behaviour) differed significantly from all other hazards, except e-mail address. E-mail address (more precautionary behaviour) differed significantly from the remaining hazards, except restricted list of 'friends' and block users.

As we studied risk perception of both security and privacy (in contrast to previous research), we also compared precautionary behaviour for the different (as in Facebook) grouped types of security- and privacy-related hazards. Repeated-measures ANOVA (see also Figure 2) showed that the effect of hazard category (security/access to account, security/information access, privacy/regulation of information-sharing, and privacy/regulation of others' information-sharing) on precautions was significant, F (3, 600) = 63.64, $p < .001$, $\varepsilon^2 = .17$. Follow-up tests with Bonferroni correction showed that security hazards related to information access met with more precautions than security hazards related to access to account, t (200) = 5.49, $p < .001$, $d = 0.21$. Privacy hazards related to regulation of information-sharing met with more precautions than privacy hazards related to regulation of others' information-sharing, t (200) = 12.78, $p < .001$, $d = 0.82$. Regulation of information-sharing also met with more precautions than both information access, t (200) = 7.29, $p < .001$, $d = 0.59$, and access to account, t (200) = 10.54, $p < .001$, $d = 0.86$.

6.2 Predicting perceived risk and precautionary behaviour

In relation to *Research Question 3*, we analysed the antecedents of security- and privacy-related risk perception in Facebook. In the analysis of perceived risk, two levels can be distinguished: hazard (at Level 1, 16 hazards, corresponding with security- and privacy settings in Facebook, existed) and subject (or participant; at Level 2, 201 participants existed). In relation to different analysis levels (non-aggregated [e.g., individual respondent] and aggregated [e.g., group]), Pedhazur (1997) points out that *cross-level* inferences (interpreting the results obtained at one level [e.g., group] to apply to another [e.g., individual]) "may be, and most often are, fallacious and grossly misleading" (p. 677). Moreover, Tabachnick and Fidell (2013) discuss the *ecological fallacy*: analysing only aggregated data (at a higher level) and then interpreting the results at a higher level to apply to a lower level. In order to avoid cross-level inferences and the ecological fallacy, multi-level analysis was performed, with perceived risk as the numeric dependent variable and the remaining variables (nine risk dimensions as well as attitudes and demographics [see Section 4]) as predictors.[3] The predictor set was constrained through an analysis of correlations between demographics and perceived risk, with a cut-off point of .10. Only average duration of Internet session exceeded this cut-off. For comparison with previous research (Garg & Camp, 2015), who tested their model of perceived

[3] The analysis did not include subject (participant) as a random effect. This is because (1) including this random effect substantially inflated the correlation between actual and predicted scores on the dependent variable and (2) the finding of a significant random effect of subject is expected and not of interest.

risk with multiple-regression analysis, Online Appendix OA2 presents corresponding results of aggregated multiple-regression analysis. The difference in results with those of multi-level analysis clearly demonstrates the fallacy of cross-level inferences and the benefit of conducting non-aggregated analysis.

In staged model-testing (recommended by Tabachnick & Fidell [2013]), the difference between subsequent models was tested (Table 7). A model with hazard-related Level-1 predictors (Model 2) explained more variance than the null model (without predictors) (Model 1). Model 3 (Model 2 augmented with interaction effects of hazard with the remaining Model-2 predictors) did not explain significantly more variance than Model 2. However, Model 4 (Model 2 augmented with Level-2 variables) explained significantly more variance than Model 2. Model 5 (Model 4 augmented with interaction effects of hazard with Level-1 predictors) explained significantly more variance than Model 3 and marginally significantly more than Model 4. Therefore, Model 5 was retained as the final model. The following results are those observed in this final model (Table 8).

Significant predictors were average duration of Internet session, attitude towards using Facebook, voluntariness (over all hazards), dread (over all hazards), hazard, catastrophic potential (hazard-specific) by hazard, and dread (hazard-specific) by hazard. Specifically, the results show that the higher dread (over all hazards), the higher perceived risk; the lower positive attitude towards sharing information on Facebook and the lower voluntariness (over all hazards), the higher perceived risk. The effects of hazard-specific catastrophic potential and dread were moderated by and therefore varied with hazard.[4] Moreover, those who spent several hours per Internet session perceived risk to be higher than those in any of the other brackets of session length.

As in previous analyses (see Section 5.1), hazards also differed in perceived risk, but here we show that this is the case even with duration of Internet session,

[4] Follow-up regression analyses per hazard (Table OA1, Online Appendix OA2) were conducted. Most consistent were the effects of the negative predictor attitude and the positive predictor dread. The results show that the positive predictor catastrophic potential was particularly influential for others posting and blocking event invitations; dread was particularly influential for login notifications, app passwords, trusted contacts, future-post-sharing, old-post-sharing, e-mail-sharing, phone number-sharing, others posting, post-sharing (tagged in), restricting posts and blocking event invitations.

attitudes towards sharing information, and perceptions of other risk dimensions, both over all hazards and hazard-specific held constant. Moreover, the effect of risk dimension varied depending on level of aggregation (over all hazards or hazard-specific). For example, voluntariness had a negative influence at the level of hazard, but not at the level of participant. There was also evidence of a composition effect of dread.[5] Dread had a positive effect at the level of participant, but at the level of hazard its effect varied with hazard.

In relation to *Research Question 4*, we analysed the antecedents of precautionary behaviour against security- and privacy-related risk in Facebook. Although none of the demographics exceeded the cut-off point of .10, duration per Internet session was retained as a potential predictor, as it was a predictor of perceived risk in the previous analysis. In the analysis of precautionary behaviour, two levels can be distinguished: hazard (at Level 1, 16 hazards existed) and subject (or participant; at Level 2, 201 participants existed). As the outcome variable was binary, multi-level analysis was performed, with precautionary behaviour (choosing a [relatively] safe setting for privacy and security hazards) as the dependent variable and the remaining variables as predictors.[6] To demonstrate the fallacy of cross-level inferences, Online Appendix OA3 presents corresponding results of aggregated multiple-regression analysis.

In staged model-testing (recommended by Tabachnick & Fidell, 2013), the difference between subsequent models was tested (Table 9). A model with hazard-related Level-1 predictors (Model 2) explained more variance than the null model (Model 1). Model 3 (Model 2 augmented with interaction effects of hazard with the remaining Model-2 predictors) explained significantly more variance than Model 2. However, Model 4 (Model 2 augmented with Level-2 variables) also explained significantly more variance than Model 2. Model 5 (Model 4 augmented with interaction effects of hazard with all Level-1 predictors) explained significantly more variance than Model

[5] A composition effect is the extent to which the relationship at a higher level adds to or differs from the relationship at a lower level (Heck, Thomas & Tabata, 2010).

[6] Again subject (participant) was not included as a random effect (1) in order to avoid substantial inflation of the correlation between taking precautions and the predicted probability of taking precautions and (2) because the finding of a significant random effect of subject is expected and not of interest

3 and Model 4. Therefore, Model 5 was retained as the final model. The following results are those observed in this final model (Table 10).

Significant predictors were average duration of Internet session, perceived risk (over all hazards), control (over all hazards), hazard, voluntariness (hazard-specific), perceived risk (hazard-specific) by hazard, and knowledge to science (hazard-specific) by hazard. Specifically, the results show that the higher risk (over all hazards) and voluntariness (hazard-specific), the greater the odds of precautionary behaviour; the lower control (over all hazards), the greater the odds of precautionary behaviour. The effects of hazard-specific perceived risk and knowledge to science were moderated by and therefore varied with hazard.[7] Moreover, for those who spent about 30 minutes and for those who spent about 45 minutes per Internet session the odds of precautionary behaviour were higher than for those spending several hours.

Some further observations are worth noting here. As in previous analyses (see Section 5.1) hazards also differed in precautionary behaviour, but here we show that this is the case even with average duration of Internet session, attitudes towards sharing information, and perceptions of other risk dimensions, both over all hazards and hazard-specific held constant. Moreover, the effect of risk dimension varied depending on level of aggregation (over all hazards or hazard-specific). For example, risk had a positive influence at the level of participant, but not at the level of hazard; however, the opposite was true for voluntariness. Moreover, control had a negative influence at the level of participant, but not at the level of hazard. Although in the previous analysis attitude towards sharing information on Facebook was a significant negative predictor of perceived risk it was marginally significant as a negative predictor of precautionary behaviour.

6.3 Summary of results

The analysis of hazards showed significant variation among hazards in perceived risk, benefit, other risk dimensions (voluntariness, immediacy of effect, knowledge

[7] Follow-up logistic regression analyses per hazard (Table OA2, Online Appendix OA3) were conducted. The results show that the positive predictor perceived risk was particularly influential for old-post-sharing, e-mail-sharing, and post-sharing (tagged in); knowledge to science was particularly influential for login notifications and post-sharing (tagged in).

about risk by affected population, knowledge about risk by science, control over risk, newness, (chronic-)catastrophic potential and dread) and precautionary behaviour. Facebook users perceived privacy hazards related to regulation of information-sharing as riskiest and privacy hazards related to regulation of others' information-sharing as least risky. Precautionary behaviour was most frequent for regulation of information-sharing and least frequent for privacy hazards related to regulation of others' information-sharing and access to account.

Significant positive predictors of students' risk perceptions were dread, catastrophic potential and length of Facebook session; significant negative predictors were attitude towards sharing information on Facebook and voluntariness (see also Table 1). Significant positive predictors of precautionary behaviour were perceived risk and voluntariness;[8] significant negative predictors of precautionary behaviour were control and length of Facebook session (see also Table 2).

7 Discussion

The aim of this research is to study security- and privacy-related risk perceptions and precautionary behaviour in social-network use. Our goals are to (1) determine how different potential security- and privacy-related hazards in an online social network are perceived, (2) establish to the extent to which people take precautions against different potential security- and privacy-related hazards, and (3) ascertain the antecedents of risk perception and precautions taken against risk of security- and privacy violations. We first discuss our findings on variation among hazards, and the prediction of perceived risk and precautionary behaviour in relation to existing work. We then discuss implications of our work, make recommendations, and present limitations of this work and ideas for future work.

7.1 Risk perception of hazards and precautionary behaviour

Although previous research (Garg & Camp, 2015) analysed students' risk perceptions of Facebook security and privacy hazards, differences among hazards

[8] We consider the finding that voluntariness (hazard-specific) was a statistical significant positive predictor of precautionary behaviour as a consequence of suppression. This is because the bivariate correlation between voluntariness and precautionary behaviour was negative (r = -0.03) and not significant. Therefore, further interpretation of this predictor is precluded.

were not statistically tested. Our results are novel as we statistically test differences, not only in terms of perceived risk, but also other risk dimensions and precautionary behaviour.

Perceptions of risk and dread were highest and precautionary behaviour was most common for regulation of information-sharing hazards related to privacy settings. The specific hazards/activities that were judged most risky were cyber-bullying, sharing telephone number (consistent with Acquisti & Gross's [2006] results on privacy concern), sharing e-mail address and failing to (have made arrangements to) receive 'login notifications'. The high risk score of cyber-bullying is not surprising (see also Van Schaik et al., 2017), as it can be seen as a direct psychological and/or physical threat, and as a consequence rather than as an action. In addition, news reports in the media of cyber-bullying may lead to high availability (Kahneman, 2011) and cyber-bullying may be associated with strong negative feelings (Finucane et al., 2000), both adding to a high degree of perceived risk or being targeted by a social-engineering attack. Sharing telephone number and sharing e-mail address do not pose a direct threat, but the information that is being shared can lead to the sharing social-media user, for example, becoming the subject of cyber-bullying. Similarly, without login notifications a social-medium user may not be aware of other users accessing their account; however, as a result, the accessed information can lead to users getting fired, getting arrested or being refused insurance when they allow posts that include compromising information to be shared with others.

Overall, perceived risk and the extent of precautionary behaviour were greater for privacy hazards related to regulation of information-sharing than hazards related to the other three categories (security/account access, security/information access and privacy/regulation of others' information-sharing). This may be because potential negative consequences of a lack of regulation of information-sharing have higher availability than those of other types of hazard. For example, it is straightforward to imagine that once a person with malicious intent has acquired a Facebook user's phone number or e-mail address they can use this information to harass the user. The effect sizes in favour of privacy/information-sharing were greater for precautionary behaviour (large or medium to large) than for perceived risk (small or small to medium), so precautionary behaviour is a more sensitive measure. This may be because precautionary behaviour for a particular Facebook setting requires that Facebook users are aware of the setting, are concerned about security or privacy in relation to the setting and can find the setting in the user-interface. However, answering a risk rating question does not require any of these; therefore, the range of ratings may be smaller than that of precautionary behaviour.

7.2 Antecedents of risk perception and precautionary behaviour

Previous research tested the predictive power of risk dimensions for perceived risk in Facebook security or -privacy (Garg & Camp, 2015), but this work suffered from aggregated data analysis. Moreover, there seems to be a lack of research testing risk perception predictors of precautionary behaviour.

Risk perception. Antecedents of risk perceptions were differentiated in terms of those that were hazard-specific (Level 1) and subject-specific predictors (Level 2). Together, these were analysed using multi-level analysis (Heck et al., 2010). *Positive* predictors of perceived risk were dread (over all hazards), duration of Internet session and also dread and catastrophic potential, both hazard-specific, moderated by hazard. These findings lead us to conclude the following.

First, the higher *dread* of security and privacy hazards overall, the higher perceived risk. This is consistent with previous work (Fischhoff et al., 1978; Garg & Camp, 2015). Therefore, the more a Facebook user perceived dread in relation to security- and privacy hazards overall, the riskier they perceive specific hazards to be. This may be particularly relevant to hazards associated with information-sharing on Facebook, as reliable data on risks are hard to come by. In addition, our results show that the hazard-specific effect of the predictor dread was moderated by hazard. In particular, the effect of dread was strongest for privacy settings for regulation of information-sharing (average beta = 0.26), which had the highest mean risk ratings, and weakest for privacy settings for regulation of others' information-sharing (average beta = 0.15), which had the lowest mean risk rating. Therefore, it seems that the effect of is stronger for hazards that are perceived as riskier. In particular, these results indicate a composition effect: for privacy settings that involved regulation of information-sharing perceived risk was higher as a Facebook user's perceived dread for the specific setting increased, in addition to the positive effect of the user's perceived dread overall, across settings.

Second, those who spent several hours per *Internet session* perceived risk to be higher than those in other time brackets. Reported average duration of Internet session may be a proxy for experience in Facebook use. Consistent with this interpretation, those who are more experienced in a particular activity perceive greater risk (Lehtonen, Havia, Kovanen, Leminen & Saure, 2016), due to specific dangers that they have encountered in the past or because they may have developed a better understanding of the risks due to their experience (increased knowledge).

Third, regarding the hazard-specific effect of *catastrophic potential* (as in the domain of Internet security; Van Schaik et al., 2017), this was positive for privacy- and security hazards that restrict what other Facebook users can do to the user's Facebook content (allowing others to post, restricting post visibility and blocking event invitations). Therefore, the more catastrophic the risks associated with these hazards, the greater perceived risk. This may be because other Facebook users' behaviour introduces additional unpredictability (Omata, 2012).

Negative predictors were attitude towards sharing information on Facebook and lower voluntariness (over all hazards). These results indicate, first, that, in line with previous work (Sjöberg & Drottz-Sjöberg, 2009), the more Facebook users have a positive *attitude* towards Facebook the less they perceive the risk associated with Facebook's specific security- and privacy settings. This result is consistent with Sjöberg's (2000) claim that attitudes drive beliefs (risk perceptions) and also with the affect heuristic (Finucane et al., 2000), according which affect has a negative effect on perceived risk. In 3D virtual worlds for online learning, risk perception regarding insider threats may be explained by the affect heuristic (Farahmand & Spafford, 2013). In particular, the authors suggest that, as less experienced users will have reduced knowledge regarding cyber-security, they will rely more affect than on logical risk analysis to make judgements about risk. Both in 3D virtual worlds and in social media, the power of the affect heuristic to influence risk perception may be further increased by a lack of reliable data on risks.

Second, (as in the domain of Internet security; Van Schaik et al., 2017) the less *voluntary* a Facebook user perceives exposure to security- and privacy hazards overall to be, the riskier they perceive specific hazards to be. This finding provides supports for the idea that the more voluntary risks are perceived to be the less risky they are perceived to be (Starr, 1969). This is in particular important in the use of social networks such as Facebook, as their use may normally be seen to be voluntary, so risk perception may be reduced. This, in turn, could then result in risk underestimation and consequently in less safe online behaviour on the network (Huang et al., 2011).

Precautionary behaviour. In our multi-level analysis, perceived risk (over all hazards) was a *positive* predictor of precautionary behaviour. The more Facebook users perceived *risk* associated with Facebook security- and privacy hazards overall, the more likely was it that they had chosen safe privacy- and security settings. This finding is consistent with the idea that perceived risk is an important predictor of precautionary behaviour in its own right (Huang et al., 2011; Keith et al., 2013) and with the role of perceived risk as an important factor in models of risk-related behaviour (Anderson & Agarwal, 2010; Liang & Xue, 2010).

The effect of the predictor hazard-specific perceived risk was moderated by hazard. The predictor was strongest and positive for privacy settings that involved information-sharing. The results indicate a composition effect: for each of these settings, precautionary behaviour was more likely as a Facebook user's perceived risk for the specific setting increased, in addition to the positive effect of the user's perceived risk overall, across settings.

Negative predictors of precautionary behaviour were control (over all hazards) and length of Internet session. First, according to previous work (Adams, 2012), in general when people feel in *control* they act less cautiously. Our results support this idea (as in the domain of Internet security; Van Schaik et al., 2017), the more a Facebook user felt in control in relation to security- and privacy hazards overall, the less likely they were to have chosen specific safe privacy- and security settings.

Second, average duration of Internet session was a significant predictor, with those who spent 30 or 45 minutes per Internet session (and who may therefore be deemed less experienced social-media users) acting with more precaution than those spending several hours. Similarly, Rosenboim et al. (2012) found a reduction in precautionary behaviour with those who were more experienced. On the one hand, according to the 'personal experience hypothesis', people become less sensitive to specific risks they face, as a result of experiencing similar events (Yechiam, Barron

& Erev, 2005). Moreover, more experience may result in greater availability and thereby elevated risk perception (Kahneman, 2011). An important difference between Yechiam et al.'s work and our study is that in the former (objectively and, even more important, subjectively based on their experience) participants could not control the hazards (missile attacks), whereas in the latter participants could fully control the hazards (Facebook security- and privacy settings). In any case, our findings demonstrate that more experienced users perceive greater risk (because of greater experience), but take fewer precautions (because of desensitisation) indicating the need for verification in further research. Alternatively, perhaps more experienced users take other precautions than the ones that we measured. For instance, consistent with our finding that control was a negative predictor of precautionary behaviour, they may control the information they reveal on Facebook to avoid breaches of privacy (Acquisti & Gross, 2006) or delete tags and photos (Young & Quan-Haase, 2013).[9] Otherwise, trust could provide an explanation for the findings: experienced users may have fewer Facebook contacts ('friends') whom they trust or experienced users may have built considerable trust in their contacts over considerable time as a Facebook user. In either case, as a consequence, experienced users' perceived need for precautionary behaviour and their actual precautionary behaviour may be reduced.

7.3 Implications

The specific aim of this research is to study security- and privacy-related risk perceptions and precautionary behaviour in social-network use. A major methodological advance over previous work that aimed to predict risk perceptions in social media is our use of non-aggregated analysis (see Van Schaik et al. [2017] for another application of this analysis in the domain of Internet security). Our results of this analysis identify significant antecedents and consequents of risk perception at different levels (hazard-specific and over hazards). This way, we avoid the ecological fallacy of aggregated analysis, which is incomplete and can be misleading

[9] The effect of the positive predictor knowledge to science (hazard-specific) was moderated by hazard. However, no particular pattern was found, with the predictor for individual hazards mostly not significant and either positive or negative.

(Tabachnick & Fidell, 2013). From our results, we draw the following practical implications.

Implications from analysis of differences between hazards. Although perceived risk and precautionary behaviour was lower for the four Facebook privacy settings for the regulation of others' information-sharing (see Table 4), they may still be precursors of direct threats. Therefore, interventions to promote risk awareness should especially target each of these as well.

Furthermore, security hazards associated with access to Facebook account were perceived as riskiest and evoke less precautionary behaviour (less than 40% of participants) (see Tables 2 and 4) than privacy hazards associated with information-sharing (more than 75%). Therefore, interventions to promote risk awareness should especially target each of these.

Implications from analysis of predicting perceived risk. Based on our results of multi-level analysis to predict perceived risk (see Table 8), interventions to promote risk awareness of information-sharing should (1) especially target Facebook users who have a more positive attitude towards using social media and those who spend less time per Internet session; (2) in general, emphasize dread associated with hazards of information-sharing; (3) in general, emphasize hazards of information-sharing even if they are seen as voluntary; (4) emphasize the catastrophic potential of particular hazards of information-sharing[10]; and (5) emphasize dread associated with particular hazards of information-sharing[11].

Implications from analysis of predicting precautionary behaviour. Based on our results of multi-level analysis to predict precautionary behaviour (see Table 10), risk interventions to promote precautionary behaviour in relation to information-sharing on social media should (1) especially target Facebook users who spend the most time per Internet session; (2) in general, emphasize risks to users' security and privacy associated with information-sharing; (3) in general, emphasize the potential threat of any hazards of information-sharing even if they are seen as controllable; (4)

[10] allowing others to post on one's timeline, failing to restrict posts and failing to block event invitations

[11] failing to set up login notifications, failing to set up trusted contacts, allowing the sharing of future posts, olds posts, e-mail address, and phone number, allowing others to post on one's timeline, allowing post-sharing (tagged in), failing to restrict posts and failing to block event invitations

emphasize the potential threat of individual hazards of information-sharing even if they are seen as involuntary; (5) emphasize the risk of particular hazards of information-sharing[12]; and (6) emphasize the importance of acting with precaution in relation to particular hazards of information-sharing even if they are well understood by science[13]. Moreover, as our results show that perceived risk is an important predictor of precautionary behaviour, the implications from the former are linked to the latter. In other words, interventions that target perceived risk should thereby indirectly also impact on and benefit precautionary behaviour. However, it is important to consider that interventions emphasizing threat under low-efficacy conditions have almost no or even negative effects on behaviour (Kok, Bartholomew, Parcel, Gottlieb & Fernández, 2014). Therefore, interventions also need to boost users' self-efficacy beliefs and response efficacy (Jansen & Van Schaik, 2017). Another consideration is the apparent mismatch between increased perceived risk and reduced precautionary behaviour in experienced Facebook users. A solution could be to 'resensitise' experienced users to Facebook security- and privacy hazards by emphasising both risk and self-efficacy (specifically by persuading them with straightforward effective actions to enhance their security and privacy on Facebook).

Different types of intervention are available to promote precautionary behaviour (Van Schaik et al., 2017). These include education-based interventions (Caputo, Pfleeger, Freeman & Johnson, 2014), marketing-linked interventions (Reid & Van Niekerk, 2016) and interventions using specific *design* features (Coventry, Briggs, Jeske & van Moorsel, 2014). We illustrate potential specific interventions with hazards privacy settings for regulation of others' information-sharing (see Table 3). In a marketing intervention (Reid & Van Niekerk, 2016), members of the target population of Facebook users may receive persuasive messages, warning of specific potential negative consequences of allowing others control of information-sharing on one's timeline. After all, when risks are underestimated it can encourage people to demonstrate unsafe behaviour (Huang et al., 2011). In an education intervention (Caputo et al., 2014), users may develop knowledge about potential negative

[12] sharing old posts and e-mail address, and allowing post-sharing

[13] failing to have made arrangements for allowing post-sharing where the user is tagged in

consequences of allowing others control and how to prevent this in the first place by choosing appropriate Facebook privacy settings. In a design intervention (Coventry et al., 2014), a set-up program may review a user's Facebook privacy settings with the user on first-time use (and at subsequent time intervals) and at that time present the potential consequences of different privacy settings. The aim is to help inform the user to make appropriate choices as decided by the user.

7.4 Limitations and future work

A consideration regarding the generalizability of our results is the type of online social network studied. We examined the online personal social network Facebook. Another major system, LinkedIn, is an online professional social network. Twitter can be seen as a personal social network or a microblog, although it is seen mainly as an information network.[14] We would expect our results potentially not to generalize to other types of social network, given differences in purpose, context of use and functionality between these networks, with potential consequent differences in risk perception and precautionary behaviour. For example, even though our hazard items could be adapted to measure risk perception in a different professional social network, sharing a phone number with others may be cause for concern in a personal social network, but may be essential when one uses LinkedIn to get a job. However, our findings may generalize to online personal social networks other than Facebook. Therefore, future research may study the antecedents and consequents or risk perception across different types of social network and establish potential moderators.

Another limitation is that we studied Facebook users' reported security- and privacy settings. As some users did not remember some of their specific settings and because the settings that they did report may not be fully accurate, future research may produce more accurate results by analysing the actual rather than the reported settings.

Furthermore, victim status (having been a victim of a specific security- or privacy breach related to one's Facebook settings) could sensitise users to risk and the need

[14] *http://www.inc.com/issie-lapowsky/ev-williams-twitter-early-years.html?cid=em01011week40day04b*

for precautionary behaviour. Therefore, future research should consider including this status as a predictor of perceived risk and precautionary behaviour. In addition, although we identified significant predictors of risk and behaviour as outcomes, further intervention research will be needed to establish how and to what extent these predictors (as mediators) can be manipulated to enhance these outcomes. Moreover, although the protection of all social-network users' security and privacy is important, this applies even more users who are more vulnerable to potential security- and privacy hazards. While this research examined adult Facebook users, future work should consider studying specific vulnerable user groups, building on existing work such as Silva, Barbosa, Silva, Silva, Mourão and Coutinho's (2017) study of teenagers' privacy on Facebook.

8 Conclusion

Using psychometric methods in a quantitative empirical online study, we analysed Facebook users' security- and privacy-related risk perceptions and precautionary behaviour. The main contributions of our work lie in demonstrating variation between hazards in people's risk perceptions related to security and privacy in social networks; and identifying predictors of perceived risks and precautionary behaviour in Facebook use in relation to existing research in risk perception and security. The main implications are the empirical demonstration that non-aggregated data analysis can help avoid methodological fallacies and derived recommendations for behavioural interventions with regard to security and privacy in Facebook use. We encourage future research to build on our insights, as part of a larger effort to better understand the determinants of people's propensity to protect themselves from potential security- and privacy-related hazards in social media and beyond. For example, our detailed insights into the influence of risk perception on precautionary behaviour could inform the inclusion of specific risk perception dimensions in models such as protection motivation theory when applied to online security and privacy.

9 References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook* (Cambridge ed.) doi:10.1007/11957454_3

Adams, J. (2012). Managing transport risks: What works? In R. Hillerbrand, P. Sandin & M. Peterson (Eds.), *Handbook of risk theory, epistemology, decision theory. ethics, and social implications of risk* (pp. 239-264). Berlin: Springer Science Business Media.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 613-643.

Beldad, A. (2015). Sharing to be sociable, posting to be popular: Factors influencing non-static personal information disclosure on Facebook among young Dutch users. *International Journal of Web Based Communities, 11*(3-4), 357-374. doi:10.1504/IJWBC.2015.072132

Beldad, A. (2016). Sealing one's online wall off from outsiders: Determinants of the use of Facebook's privacy settings among young Dutch users. *International Journal of Technology and Human Interaction, 12*(1), 21-34. doi:10.4018/IJTHI.2016010102

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology and People, 28*(3), 426-441. doi:10.1108/ITP-10-2014-0232

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems, 39*(4), 837-864.

Bronfman, N. C., & Cifuentes, L. A. (2003). Risk perception in a developing country: The case of Chile. *Risk Analysis, 23*(6), 1271-1285. doi:10.1111/j.0272-4332.2003.00400.x

Bronfman, N. C., Cifuentes, L. A., Dekay, M. L., & Willis, H. H. (2007). Accounting for variation in the explanatory power of the psychometric paradigm: The effects of aggregation and focus. *Journal of Risk Research, 10*(4), 527-554.

Caine, K., Kisselburgh, L. G., & Lareau, L. (2011). Audience visualization influences disclosures in online social networks. *29th Annual CHI Conference on Human Factors in Computing Systems, CHI 2011,* Vancouver, BC. 1663-1668. doi:10.1145/1979742.1979825

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy, 12*(1), 28-38. doi:10.1109/MSP.2013.106

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47-56. doi:10.1016/j.dss.2015.12.007

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. *International Conference of Design, User Experience, and Usability,* 229-239.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475-487. doi:10.1006/imms.1993.1022

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. doi:10.1002/ejsp.2049

Dinev, T., McConnell, A. R., & Smith, J.H. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639-655. doi:10.1287/isre.2015.0600

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers, 15*(1), 5-15. http://dx.doi.org/10.1007/s10796-010-9265-x.

Field, A. P. (2013). *Discovering statistics using IBM SPSS statistics*. London: Sage.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences, 9*(2), 127-152. doi:10.1007/BF00143739

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. London: Taylor & Francis.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Garg, V., Benton, K. & Camp, L.J. (2014). *The privacy paradox: a Facebook case study*. 2014 TPRC conference paper.

Garg, V., & Camp, L. J. (2015). Cars, condoms, and Facebook. In Y. Desmedt (Ed.), *Information security* (pp. 280-289) Springer International Publishing.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *22nd International Conference on World Wide Web, WWW 2013,* Rio de Janeiro. 737-744.

Heck, R. H., Thomas, S. L., & Tabata, L. N. (2010). *Multilevel and longitudinal modeling with IBM SPSS*. London: Routledge Academic.

Huang, D., Patrick Rau, P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human Computer Studies, 69*(12), 870-883.

Huang, L., Ban, J., Sun, K., Han, Y., Yuan, Z., & Bi, J. (2013). The influence of public perception on risk acceptance of the chemical industry and the assistance for risk communication. *Safety Science, 51*(1), 232-240. doi:10.1016/j.ssci.2012.05.018

Jansen, J., & Schaik, P. van (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security, 25*(2), 165-180. doi:10.1108/ICS-03-2017-0018

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: It's complicated. *8th Symposium on Usable Privacy and Security, SOUPS 2012,* Washington, DC. doi:10.1145/2335356.2335369

Joinson, A. N., Reips, U., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. doi:10.1080/07370020903586662

Kahneman, D. (2011). *Thinking fast, thinking slow*. London: Penguin.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies, 71*(12), 1163-1173. doi:10.1016/j.ijhcs.2013.08.016

Kim, K. H., Choi, J. W., Lee, E., Cho, Y. M., & Ahn, H. R. (2015). A study on the risk perception of light pollution and the process of social amplification of risk in Korea. *Environmental Science and Pollution Research,* doi:10.1007/s11356-015-4107-5

Kok, G., Bartholomew, L. K., Parcel, G. S., Gottlieb, N. H., & Fernández, M. E. (2014). Finding theory- and evidence-based alternatives to fear appeals: Intervention mapping. *International Journal of Psychology, 49*(2), 98-107. doi:10.1002/ijop.12001

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security, 64*, 122-134. doi:10.1016/j.cose.2015.07.002

Layte, R., McGee, H., Rundle, K., & Leigh, C. (2007). Does ambivalence about becoming pregnant explain social class differentials in use of contraception? *European Journal of Public Health, 17*(5), 477-482. doi:10.1093/eurpub/ckl263

Lehtonen, E., Havia, V., Kovanen, A., Leminen, M., & Saure, E. (2016). Evaluating bicyclists' risk perception using video clips: Comparison of frequent and infrequent city cyclists. *Transportation Research Part F: Traffic Psychology and Behaviour, 41*, 195-203. doi:10.1016/j.trf.2015.04.006

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association of Information Systems, 11*(7), 394-413.

Malin, B., & Sweeney, L. (2001). *Re-identification of DNA through an automated linkage process*. In Proceedings of the AMIA Symposium (pp. 423-427). American Medical Informatics Association.

Morton, A., & Sasse, M. A. (2012). Privacy is a process, not a PET a theory for effective privacy practice. *2012 21st New Security Paradigms Workshop, NSPW 2012,* Bertinoro. 87-104.

Omata, K. (2012). Effects of the predictability and controllability of crime on criminal risk perception and fear of crime in Japanese students. *The Japanese Journal of Social Psychology, 27*(3), 174-184.

Pedhazur, E. (1997). *Multiple regression in behavioral research: Explanation and prediction* (3rd ed.). London: Harcourt Brace.

Reid, R., & Van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security, 24*(2), 177-193. doi:10.1108/ICS-01-2016-0003

Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security, 31*(2), 221-232. doi:10.1016/j.cose.2011.12.001

Rosenboim, M., Benzion, U., Shahrabani, S., & Shavit, T. (2012). Emotions, risk perceptions, and precautionary behavior under the threat of terror attacks: A field study among Israeli college students. *Journal of Behavioral Decision Making, 25*(3), 248-256. doi:10.1002/bdm.728

Saridakis, G., Benson, V., Ezingeard, J., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320-330. doi:10.1016/j.techfore.2015.08.012

Schaik, P. van, Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559. doi:10.1016/j.chb.2017.05.038

Schneier, B. (2015). *Secrets and lies: Digital security in a networked world (15th-anniversary edition)*. Hoboken, New Jersey: John Wiley & Sons.

Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428-438. doi:10.1016/j.intcom.2010.05.001

Silva, C. S., Barbosa, G. A., Silva, I. S., Silva, T. S., Mourão, F., & Coutinho, F. (2017, June). Privacy for children and teenagers on social networks from a usability perspective: a case study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference* (pp. 63-71). ACM.

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological Review, 63*(2), 129-138.

Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis, 20*(1), 1-11. doi:10.1111/0272-4332.00001

Sjöberg, L., & Drottz-Sjöberg, B. (2009). Public risk perception of nuclear waste. *International Journal of Risk Assessment and Management, 11*(3-4), 264-296.

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280-285.

Slovic, P., MacGregor, D., & Kraus, N. N. (1987). Perception of risk from automobile safety defects. *Accident Analysis and Prevention, 19*(5), 359-373.

Starr, C. (1969). Social benefit versus technological risk. *Science, 165*(3899), 1232-1238.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Boston, MA; London: Pearson.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-Disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273. doi:10.1111/jcc4.12052

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Yechiam, E., Barron, G., & Erev, I. (2005). The role of personal experience in contributing to different patterns of response to rare terrorist attacks. *Journal of Conflict Resolution, 49*(3), 430-439. doi:10.1177/0022002704270847

Young, L., Kuo, H., & Chiang, C. (2015). Environmental health risk perception of a nationwide sample of Taiwan college students majoring in engineering and health sciences. *Human and Ecological Risk Assessment, 21*(2), 307-326.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information Communication and Society, 16*(4), 479-500. doi:10.1080/1369118X.2013.777757

Zureik, E., & Stalker, L. H. (2010). The cross-cultural study of privacy. In E. Zureik, L. H. Stalker, E. Smith, D. Lyon & Y. E. Chan (Eds.), *Surveillance, privacy, and the globalization of personal information: International comparisons.* (pp. 8-30). Montreal: McGill-Queen's Press-MQUP.

Table 1

Predictors in relation to risk perception

Predictor	D	L1	L2
Lack of voluntariness (Starr, 1969; AC)	+		√
Lack of immediacy (Kahneman, 2011; AC)	-		
Lack of knowledge by affected population (Garg & Camp, 2015)	+		
Lack of knowledge by science (Garg & Camp, 2015)	+		
Lack of control (Adams, 2012; Rhee, Ryu & Kim, 2012; AC)	+		
Lack of newness (Schneier, 2015; Malin & Sweeney, 2001)	-		
Catastrophic potential (Adams, 2012; Acquisti & Gross, 2006; AC)	+	I	
Dread (Fischhoff et al., 1978; Garg & Camp, 2015; Schneier, 2015; AC)	+	I	√
Benefit (Finucane et al., 2000; Chakraborty, Lee, Bagchi-Sen, Upadhyaya & Raghav Rao, 2016)	-		
Attitudes (Sjöberg & Drottz-Sjöberg, 2009)	-		√
Experience/availability (Kahneman, 2011)	+		√

Note. D: expected direction of prediction. L1/L2: Test result at Level 1 (hazard)/Level 2 (participant, over hazards) in mixed-model analysis. √ Statistically significant. I: Significant interaction with hazard. AC: Author Citation 1.

Table 2

Predictors in relation to precautionary behaviour

Predictor	D	L1	L2
Risk (Boss, Galletta, Lowry, Moody & Polak, 2015)	+	I	√
Benefit	-		
Voluntariness	+	√	
Lack of immediacy	-		
Lack of knowledge by affected population	+		
Lack of knowledge by science	+	I	
Control (AC)	-		√
Lack of newness	-		
Catastrophic potential	+		
Dread	+		
Experience (Rosenboim et al., 2012)	-		√

Note. D: expected direction of prediction. L1/L2: Test result at Level 1 (hazard)/Level 2 (participant, over hazards) in mixed-model analysis. √ Statistically significant. I: Significant interaction with hazard. AC: Author Citation 1.

Table 3

Hazards and comparison activities studied

Hazard/comparison activity		Default setting in Facebook[a]	Protection provided by default[b]
Related to security settings for access to Facebook account			
1	Failing to do ‘secure browsing’	Off (i.e., not allowing yourself ‘secure browsing’)	Poor
2	Failing to (have made arrangements to) receive ‘login notifications’	None (i.e., not allowing yourself ‘login notifications’)	Poor
3	Failing to use ‘app passwords’	None (i.e., not allowing yourself ‘app passwords’)	Poor
4	Failing to use ‘trusted contacts’	None (not allowing yourself ‘trusted contacts’)	Poor
Related to privacy settings/tools for user’s regulation of information-sharing			
5	Allowing all your future posts to be shared with others	Friends	Neutral
6	Allowing all your old posts to be shared with others	Off (if this attribute [Limit Past Posts] is switched on, old posts will only be shared with friends)	Good
7	Allowing your e-mail address to be shared with others	Everyone	Poor
8	Allowing your phone number to be shared with others	Everyone	Poor
Related to privacy settings/tools for user’s regulation of others’ information-sharing			
9	Allowing others to post on your timeline	Friends	Neutral
10	Failing to review friends’ posts before they appear on your timeline; these are posts in which a link to your profile is included	Off (i.e., not allowing yourself to review posts ‘friends’ tag you in before they appear on your timeline)	Poor
11	Allowing others’ posts to be shared on your timeline; these are posts in which others have included a link to your profile	Friends of friends	Poor/neutral
12	Failing to review links that appear in your posts; these are links to others’ Facebook profile that others have inserted before they appear on Facebook	Off (i.e., not allowing yourself to review tags people add to your post before tag appears on Facebook)	Poor
Related to security settings for access to shared information in Facebook			
13	Failing to keep a restricted list of ‘friends’ who can only see the information and posts that you make public	None (i.e., not having a restricted list …)	Poor
14	Failing to block users so they can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you or add you as a ‘friend’	None (i.e., not allowing yourself to block …)	Poor

15	Failing to block event invitations	None (i.e., not allowing yourself to block …)	Poor
16	Failing to block apps, so they can no longer contact you or get non-public information about you through Facebook	None (i.e., not allowing yourself to block …)	Poor
Comparison activity			
17	Browsing Internet sites for information		
18	Cyber-bullying		

[a]at the time of data collection (April 2014). [b]Our assessment; see also Section 6.1.

Table 4
Means for risk and risk balance

	Risk			Risk balance		
	Mean	*CI* .95		Mean	*CI* .95	
Hazard		Lower limit	Upper limit		Lower limit	Upper limit
Security/access to Facebook account						
1 Secure browsing	4.91	4.69	5.12	-1.53	-1.89	-1.17
2 Login notifications	5.23	5.02	5.43	-1.94	-2.31	-1.57
3 App passwords	4.86	4.65	5.07	-1.24	-1.55	-0.94
4 Trusted contacts	4.55	4.33	4.76	-0.98	-1.27	-0.68
Privacy/information-sharing						
5 Allowing future post-sharing	4.88	4.67	5.09	-1.24	-1.55	-0.94
6 Allowing old post-sharing	4.84	4.63	5.05	-1.40	-1.70	-1.09
7 Allowing e-mail sharing	5.19	4.97	5.41	-1.81	-2.17	-1.45
8 Allowing phone-sharing	5.38	5.15	5.62	-2.26	-2.64	-1.88
Privacy/timeline and tagging						
9 Allowing others posting	4.50	4.27	4.72	-0.74	-1.07	-0.40
10 Reviewing posts	4.49	4.30	4.68	-0.97	-1.25	-0.68
11 Allowing post-sharing	4.53	4.33	4.73	-0.79	-1.08	-0.49
12 Reviewing tags	4.42	4.22	4.63	-1.02	-1.31	-0.74
Security/access to information-sharing						
13 Restricting posts	4.88	4.65	5.10	-1.36	-1.70	-1.03
14 Blocking users	4.66	4.44	4.87	-1.06	-1.37	-0.75
15 Blocking event invitations	4.07	3.84	4.30	-0.47	-0.78	-0.15
16 Blocking apps	4.62	4.39	4.85	-0.97	-1.29	-0.64
Comparison activity						
17 Internet browsing	3.56	3.35	3.77	1.86	1.55	2.16
18 cyber-bullying	5.60	5.41	5.79	-2.82	-3.18	-2.45

Table 5
Mean ratings on perceived risk and other dimensions of risk, sorted by perceived risk

	Risk	Benefit	Voluntariness	Immediacy of effect	Knowledge (population)	Knowledge (science)	Control over risk	Newness	Catastrophic potential	Dread
Cyber-bullying	5.60	2.79	4.62	3.28	4.10	3.71	4.03	4.21	4.71	5.12
Phone number	5.38	3.12	3.55	3.67	3.98	3.76	5.13	4.61	3.87	4.77
Login notifications	5.23	3.29	3.89	3.69	4.21	3.77	4.77	4.12	3.82	4.58
E-mail address	5.19	3.38	3.54	3.75	4.02	3.69	5.03	4.60	3.65	4.68
Secure browsing	4.91	3.38	3.70	3.92	4.16	3.76	4.96	4.43	3.80	4.19
Future posts	4.88	3.64	3.43	4.16	4.29	4.03	4.90	4.34	3.80	4.05
Restricted list of 'friends'	4.88	3.51	3.38	3.92	4.14	3.97	5.00	4.41	3.77	4.02
App passwords	4.86	3.62	3.51	4.09	4.46	4.00	5.01	4.08	3.68	4.16
Old posts	4.84	3.44	3.56	4.02	4.21	4.03	4.94	4.59	3.76	3.95
Block users	4.66	3.60	3.46	3.83	4.27	3.78	4.97	4.27	3.83	4.02
Block apps	4.62	3.65	3.62	3.91	4.20	3.91	4.86	4.17	3.74	4.00
Trusted contacts	4.55	3.57	3.46	4.20	4.36	4.04	4.89	3.99	3.66	4.03
Post-sharing	4.53	3.74	3.62	3.93	4.15	4.04	4.73	4.23	3.74	3.85
Others posting	4.50	3.76	3.54	3.68	4.10	3.94	4.88	4.38	3.72	3.78
Post review	4.49	3.52	3.64	3.83	4.19	4.03	4.79	4.40	3.72	3.92
Tag review	4.42	3.40	3.54	3.95	4.20	4.07	4.81	4.23	3.76	3.87
Block events	4.07	3.60	3.42	3.94	4.37	3.90	5.03	4.26	3.59	3.71
Browsing Internet	3.56	5.42	3.19	3.82	3.81	3.50	5.00	5.10	3.49	3.01

Table 6

Precautionary behaviour in relation to hazards, sorted by precaution taken

	Precaution taken	Precaution not taken	Precaution unknown
Phone number	72	17	11
E-mail address	65	22	13
List of 'friends'	58	27	15
Block users	55	26	18
'Secure browsing'	50	20	30
Old posts sharing	44	26	29
Block apps	44	28	28
New posts sharing	43	29	28
'Login notifications'	42	29	28
Post-sharing	37	37	26
Block event invitations	37	42	20
Others posting in timeline	34	48	17
Review tags	34	41	25
'Trusted contacts'	34	46	20
Review posts	32	44	24
'App passwords'	26	46	27

Note . Numbers are percentages. Not all row totals add up to 100% because of rounding.

Table 7

Model testing, dependent variable perceived risk

	Model	df	-2LL	*r* (pv, risk)
1	Null model	2	12058.97	0.00
2	Level-1 predictors[a]	26	11630.60	0.35
3	Level-1 predictors and interactions with hazard	161	11472.37	0.41
4	Level-1 and Level-2 predictors[b]	40	11363.61	0.44
5	Level-1 and Level-2 predictors and interactions with hazard	175	11200.98	0.48

Test of model difference				
Model difference	chi square	*df*	*p*	Δ*r* (pv, risk)
M1 - M2	428.37	24	0.000	0.35
M1 - M3	586.60	159	0.000	0.41
M1 - M4	695.36	38	0.000	0.44
M1 - M5	857.99	173	0.000	0.48
M2 - M3	158.23	135	0.084	0.06
M2 - M4	266.99	14	0.000	0.09
M3 - M5	271.39	14	0.000	0.08
M4 - M5	162.63	135	0.053	0.04

Note . pv: predicted value. Null model: intercept only. Level 1: hazard. Level 2: subject (participant).

[a] hazard, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential and dread

[b] average duration of Internet session and attitude towards the use of Facebook as well as, averaged over hazards, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential and dread

Table 8

Parameter estimates and tests of effects, dependent variable perceived risk

Parameter	*b*	*CI* 95%		*df1*	*df2*	*F*	*p*
		LL	*UL*				
Level 2/subject							
Av. duration of Internet session				4	3216	17.67	**<0.001**
From 1 to about 15 minutes vs several hours	*-0.47*	-0.65	-0.29	1	3216	27.01	**<0.001**
About 30 minutes vs several hours	*-0.22*	-0.36	-0.08	1	3216	8.89	**0.003**
About 45 minutes vs several hours	*-0.73*	-0.92	-0.53	1	3216	53.86	**<0.001**
About 1 hour vs several hours	*-0.17*	-0.30	-0.05	1	3216	7.48	**0.006**
Attitude towards Facebook use	*0.19*	0.15	0.23	1	3216	90.15	**<0.001**
Benefit (subject)	-0.06	-0.12	0.01	1	3216	2.81	0.094
Voluntariness (subject)	*-0.09*	-0.15	-0.03	1	3216	7.83	**0.005**
Immediacy (subject)	0.05	-0.02	0.12	1	3216	2.11	0.146
Knowledge to population (subject)	0.04	-0.03	0.11	1	3216	0.98	0.322
Knowledge to science (subject)	-0.03	-0.11	0.04	1	3216	0.85	0.356
Control (subject)	0.00	-0.06	0.07	1	3216	0.01	0.904
Newness (subject)	-0.03	-0.09	0.03	1	3216	0.92	0.337
Catastrophic potential (subject)	0.02	-0.05	0.09	1	3216	0.31	0.578
Dread (subject)	*0.25*	0.18	0.32	1	3216	48.28	**<0.001**
Level 1/hazard							
Hazard				15	3216	6.58	**<0.001**
Benefit (hazard)	-0.03	-0.15	0.10	1	3216	0.16	0.690
Voluntariness (hazard)	0.09	-0.03	0.21	1	3216	2.25	0.134
Immediacy (hazard)	-0.01	-0.14	0.12	1	3216	0.02	0.887
Knowledge to population (hazard)	0.04	-0.10	0.18	1	3216	0.29	0.591
Knowledge to science (hazard)	-0.06	-0.21	0.09	1	3216	0.60	0.440
Control (hazard)	0.06	-0.08	0.19	1	3216	0.76	0.385
Newness (hazard)	0.01	-0.11	0.14	1	3216	0.04	0.839
Catastrophic potential (hazard)	0.08	-0.06	0.22	1	3216	1.16	0.281
Dread (hazard)	-0.02	-0.15	0.11	1	3216	0.07	0.795
Benefit (hazard) by hazard				15	3216	1.15	0.307
Voluntariness (hazard) by hazard				15	3216	1.38	0.145
Immediacy (hazard) by hazard				15	3216	1.10	0.352
Knowledge to population (hazard) by hazard				15	3216	1.46	0.112
Knowledge to science (hazard) by hazard				15	3216	1.05	0.403
Control (hazard) by hazard				15	3216	0.63	0.853
Newness (hazard) by hazard				15	3216	0.92	0.545
Catastrophic potential (hazard) by hazard				15	3216	1.71	**0.042**
Dread (hazard) by hazard				15	3216	1.67	**0.050**

Note . All predictors, except average duration of Internet session and hazard, are mean-centred.
Figures in bold indicate a significant test result at the 0.05 significance level.

Table 9

Model testing, dependent variable safe precautionary behaviour

	Model	df	-2LL	*r* (pp, pb)
1	Null model	1	4415.03	0.00
2	Level-1 predictors[a]	26	4120.11	0.30
3	Level-1 predictors and interactions with hazard	176	3914.22	0.39
4	Level-1 and Level-2 predictors[b]	41	4044.59	0.33
5	Level-1 and Level-2 predictors and interactions with hazard	191	3840.72	0.41

Test of model difference				
Model difference	chi square	*df*	*p*	Δ*r* (pp, pb)
M1 - M2	294.92	25	0.000	0.30
M1 - M3	500.81	175	0.000	0.39
M1 - M4	370.44	40	0.000	0.33
M1 - M5	574.31	190	0.000	0.41
M2 - M3	205.89	150	0.002	0.09
M2 - M4	75.51	15	0.000	0.03
M3 - M5	73.50	15	0.000	0.02
M4 - M5	203.87	150	0.002	0.08

Note . pb: precautionary behavior. pp: predicted probability of precautionary behavior. Null model: intercept and uniform predictor. Level 1: hazard. Level 2: subject (participant). Analysis of a null model with intercept only by the SPSS procedure GENLINMIXED produces erroneous results for -2LL that cannot be compared with subsequent models having one or more predictor. The problem was resolved by including an auxiliary uniformly distributed predictor in the null model that was correlated with neither the dependent variable nor any of the predictor variables.

[a]hazard, perceived risk, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential and dread

[b]average duration of Internet session and attitude towards the use of Facebook as well as, averaged over hazards, risk, benefit, voluntariness, immediacy, knowledge by population, knowledge by science, control, newness, catastrophic potential and dread

Table 10

Parameter estimates and tests of effects, dependent variable safe precautionary behaviour

Parameter	*OR*	*CI* 95%		*df1*	*df2*	*F*	*p*
		LL	*UL*				
Level 2/subject							
Av. duration of Internet session				4	3024	9.73	**<0.001**
From 1 to about 15 minutes vs several hours	1.08	0.81	1.43	1	3024	0.28	0.599
About 30 minutes vs several hours	*0.57*	0.45	0.72	1	3024	22.83	**<0.001**
About 45 minutes vs several hours	*0.60*	0.44	0.83	1	3024	9.87	**0.002**
About 1 hour vs several hours	1.08	0.89	1.32	1	3024	0.60	0.440
Attitude towards Facebook use	1.06	1.00	1.14	1	3024	3.46	0.063
Risk (subject)	*1.17*	1.04	1.31	1	3024	7.13	**0.008**
Benefit (subject)	1.08	0.97	1.20	1	3024	1.97	0.160
Voluntariness (subject)	0.91	0.83	1.01	1	3024	2.98	0.085
Immediacy (subject)	0.97	0.87	1.09	1	3024	0.25	0.615
Knowledge to population (subject)	0.90	0.80	1.01	1	3024	3.23	0.073
Knowledge to science (subject)	1.11	0.99	1.25	1	3024	3.24	0.072
Control (subject)	*0.88*	0.79	0.98	1	3024	5.16	**0.023**
Newness (subject)	0.96	0.87	1.05	1	3024	0.84	0.361
Catastrophic potential (subject)	1.02	0.91	1.14	1	3024	0.09	0.766
Dread (subject)	0.91	0.80	1.02	1	3024	2.67	0.102
Level 1/hazard							
Auxiliary uniformly distributed predictor	1.00	1.00	1.00	1	3024	0.04	0.841
Hazard				15	3024	8.57	**<0.001**
Risk (hazard)	0.97	0.82	1.16	1	3024	0.09	0.769
Benefit (hazard)	1.11	0.90	1.37	1	3024	0.94	0.332
Voluntariness (hazard)	*1.21*	1.00	1.45	1	3024	3.97	**0.046**
Immediacy (hazard)	0.99	0.81	1.22	1	3024	0.01	0.913
Knowledge to population (hazard)	0.98	0.79	1.22	1	3024	0.04	0.849
Knowledge to science (hazard)	1.04	0.83	1.32	1	3024	0.13	0.722
Control (hazard)	0.85	0.68	1.06	1	3024	2.09	0.148
Newness (hazard)	1.04	0.85	1.26	1	3024	0.13	0.721
Catastrophic potential (hazard)	0.96	0.77	1.19	1	3024	0.13	0.718
Dread (hazard)	1.14	0.93	1.39	1	3024	1.65	0.199
Risk (hazard) by hazard				15	3024	2.75	**<0.001**
Benefit (hazard) by hazard				15	3024	0.91	0.552
Voluntariness (hazard) by hazard				15	3024	0.62	0.860
Immediacy (hazard) by hazard				15	3024	0.96	0.496
Knowledge to population (hazard) by hazard				15	3024	0.96	0.491
Knowledge to science (hazard) by hazard				15	3024	2.06	**0.009**
Control (hazard) by hazard				15	3024	0.96	0.496
Newness (hazard) by hazard				15	3024	0.73	0.756
Catastrophic potential (hazard) by hazard				15	3024	0.91	0.551
Dread (hazard) by hazard				15	3024	1.25	0.226

Note . All predictors, except the uniformly distributed auxiliary predictor, average duration of Internet session and hazard, are mean-centred.

Analysis of a null model with intercept only by the SPSS procedure GENLINMIXED produces erroneous results for -2LL that cannot be compared with subsequent models having one or more predictor.

The problem was resolved by including an auxiliary uniformly distributed predictor in the null model that was correlated with neither the dependent variable nor any of the predictor variables.

Figure 1. Mean perceived risk by Facebook setting.

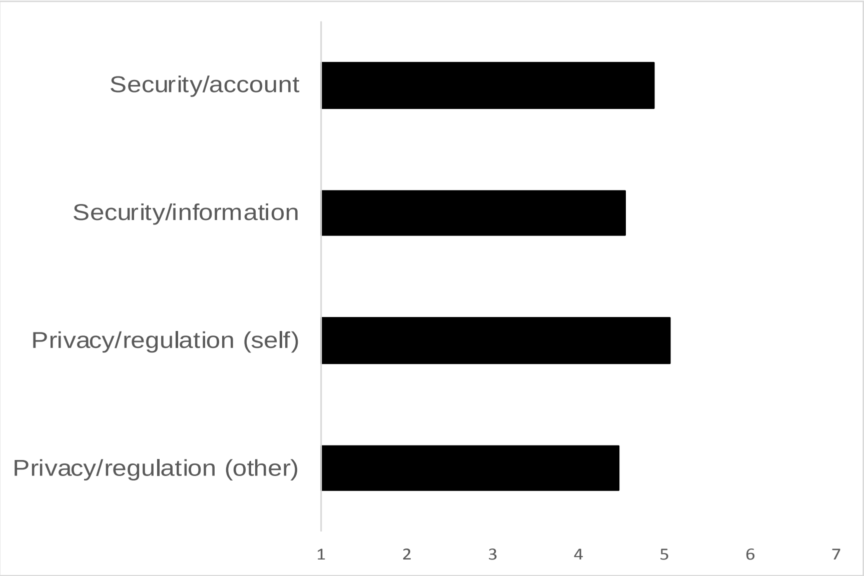
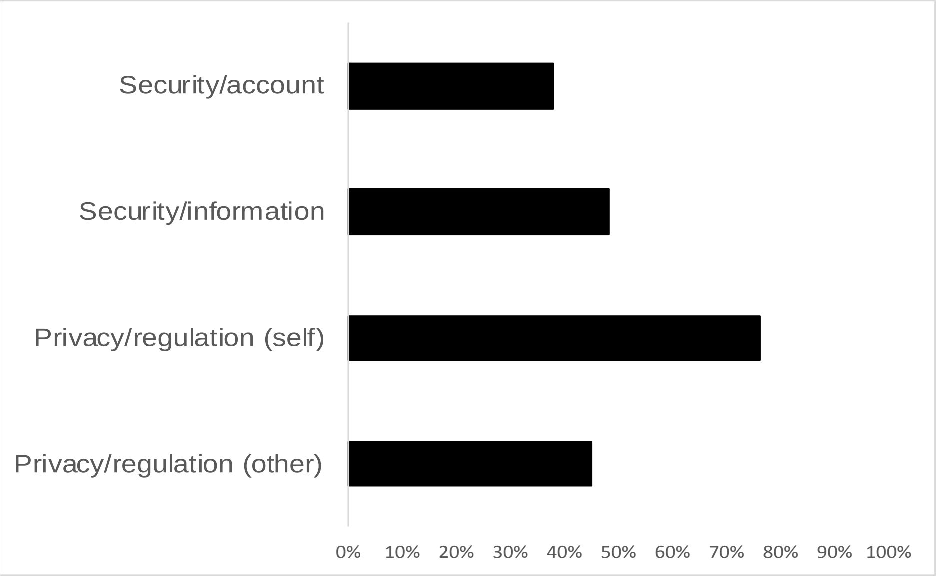


Figure 2. Precautionary behaviour by Facebook setting.


Security/account
Security/information
Privacy/regulation (self)
Privacy/regulation (other)