International Journal of Cyber Behavior, Psychology and Learning
Volume 13 • Issue 1

Are Perceptions About Government and Social Media Providers Related to Protection Motivation Online?

Simon Vrhovec, University of Maribor, Slovenia*
https://orcid.org/0000-0002-6951-6369

Damjan Fujs, University of Ljubljana, Slovenia
https://orcid.org/0000-0002-6357-8569

ABSTRACT

This study aims to explore the relations between perceptions about government and social media providers, and protection motivation of social media users. A survey was conducted among students at a public university in Slovenia (N=276). The results of PLS-SEM analysis indicate that fear of government intrusions is associated with both perceived threat and privacy concern. This establishes the perceptions about government as important factors related to both privacy concern and threat appraisal according to protection motivation literature. Non-significant relations between trust in internet service provider, and perceived threat and privacy concern indicate that social media users may not consider them as relevant cyberspace actors capable of threatening their privacy on social media. The results also suggest that trust in social media providers moderates the association between privacy concern and protection motivation. Privacy concern appears to be related to protection motivation only if trust in social media provider is high.

KEYWORDS:

Privacy Concern, Surveillance, Fear, Trusting Beliefs, Government, Internet Service Provider, ISP, Social Network, Social Media, Protection Motivation,PMT,Fear Appeal,Threat Appraisal,Coping Appraisal

INTRODUCTION

Social media are used by billions of people every day. Social media may be a powerful tool for targeting and monitoring social activity of people online (e.g., detecting social events, tackling terrorism and violent extremism) (Lee et al., 2018). Social media are also interesting for political interference (Badawy et al., 2018; Specht & Ros-Tonen, 2017), bots for mining public opinion (Woolley, 2016), spreading fake news (Sivasangari et al., 2018; Steinebach et al., 2020), and radicalization activities

DOI: 10.4018/IJCBPL.324085

*Corresponding Author

(Tundis et al., 2020). Due to their potential for tackling various societal issues, social media may be seen by their users as a hunting ground prone to government surveillance (Watt, 2021). Governments may achieve this by involving internet service providers (ISPs) in their countries. ISPs are relatively easily influenced by governments as the latter have several leverages to do so, from legislation to more direct means (i.e., direct contact between government agencies and ISPs) depending on the country.

Another way to monitor social activities of social media users is to involve social media providers. Compared to ISPs, social media providers are not as easily influenced by governments around the world simply because their infrastructure is not limited to a single country, and they operate in various countries. For example, Facebook is headquartered in the US, and banned in countries, such as China, Iran, North Korea, etc. (Comparitech, 2021; Erdbrink, 2013; Talmadge, 2016). Therefore, social media providers may have more leverage to decide whether to aid governments in their endeavors or not than ISPs. If governments are not aided by social media providers, they may still be able to use their platforms for surveillance through infiltration. Although it is known that social media providers try to tackle the spread of fake news and political interference on their platforms, little is known regarding their response to such infiltration which may still fall under the umbrella of unauthentic behavior.

Besides governments, other actors are threatening social media users in the cyberspace as well. Cybersecurity incidents and privacy violations related to social media appear to be growing as high-profile incidents seem to emerge on a regular basis (Bordoff et al., 2017; M. Xu et al., 2018). For example, the hacking of Twitter in 2013, the hacking of LinkedIn and Myspace that surfaced in 2016, and Google Plus data exposure. Such cybersecurity incidents can have considerable consequences for social media users (Uldam, 2016). These cyberthreats are complemented by those enabled by social media providers themselves, such as the Facebook – Cambridge Analytica scandal in 2018. Facebook enabled third-party companies, such as Cambridge Analytica, to create apps that could capture private data of their users. Cambridge Analytica used this feature to target particular individuals based on their profiles (Isaak & Hanna, 2018). Although the policies of social media providers changed in a way that such privacy scandals may be harder to realize, social media is still free to use because their users' data is being sold to third parties in the background (Lutz et al., 2020). Essentially, the core business model of social media providers, surveillance or data capitalism (Lutz et al., 2020), did not change.

There are three key areas of research on social media user behavior: information disclosure, privacy protecting behavior, and protection motivation. The association between privacy concern and information disclosure has been often studied both in the context of social media (Benamati et al., 2017; H. Choi et al., 2018; Fujs et al., 2019; S.-W. Lin & Liu, 2012; Mosteller & Poddar, 2017) and elsewhere online (Dinev et al., 2008; Keith et al., 2013). Similarly, there is some literature studying the association between privacy concern and privacy protecting behavior on social media (Lutz et al., 2020). Even though social media providers try to secure their users, social media users still carry the responsibility to adequately protect their own social media accounts (Jansen & van Schaik, 2018). A significant body of research studies protection motivation (e.g., implementation of recommended security measures, such as periodically changing the password, using strong passwords and paying attention to login alerts) of individuals online through the lens of fear appeals (Aurigemma et al., 2019; Vrhovec & Mihelič, 2021). According to the protection motivation theory (PMT), protection motivation is the result of threat and coping appraisal (Aurigemma et al., 2019; Floyd et al., 2000; Vrhovec & Mihelič, 2021). Nevertheless, research on protection motivation on social media seems to be particularly scarce as only a few studies investigate it (Fujs et al., 2019, 2018).

To summarize, there are three key actors monitoring the activity of social media users, namely, the government of the residing country of social media users, the ISP, and the social media provider. In this paper, we focus on social media users' perceptions on all three actors. Privacy concern has been related to trusting beliefs (Lutz et al., 2018) therefore we examine how trusting beliefs about all three actors are related to protection motivation of users on social media. We also study the relation between fear of government intrusions and protection motivation. The study is loosely based on PMT since it aims to investigate a rarely researched context therefore qualifying as an exploratory study.

This study has five key objectives: 1) to determine how trust in government and trust in ISP are related to privacy concern of social media users, 2) to study how fear of government is related to privacy concern of social media users, 3) to investigate how trust in government and trust in ISP are related to protection motivation of social media users, 4) to study how fear of government is related to protection motivation of social media users, and 5) to explore how trust in social media provider is related to both privacy concern and protection motivation.

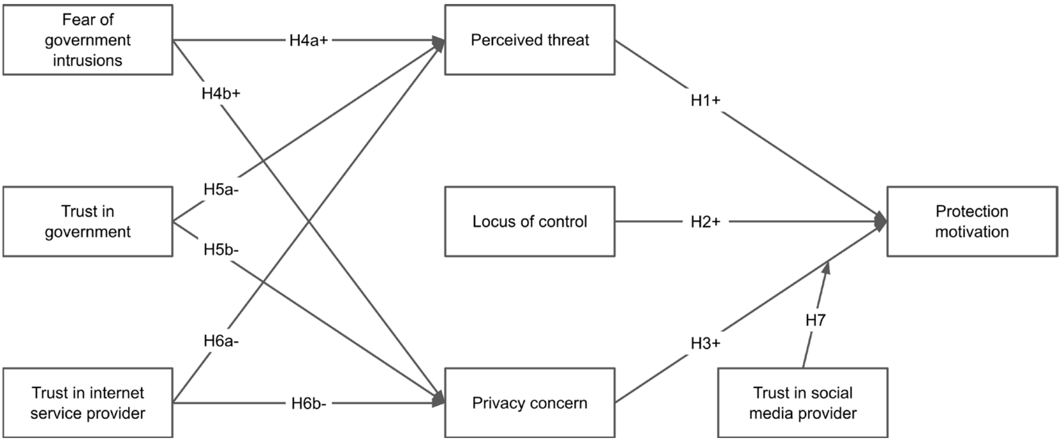
This paper makes three key contributions to the literature. First, this is one of the first studies to investigate the associations between perceptions about government (i.e., fear of government intrusions into privacy of social media users and trusting beliefs towards government and ISP) and privacy concern thus contributing to the privacy literature. Second, this study also contributes to the protection motivation literature by being one of the first to examine the associations between perceptions about government and the appraisal of the threat of intrusions into social media accounts. Third, this study advances our understanding of the association between privacy concern and protection motivation by investigating its relation to social media users' perceptions about social media provider (i.e., the moderating role of trust in social media provider) which contributes to the literature on both privacy and protection motivation on social media.

RESEARCH MODEL

In this study, we propose and empirically test a research model presented in Figure 1.

PMT is often used to explain secure behavior of individuals online (Aurigemma et al., 2019; Jansen & van Schaik, 2018; Johnston & Warkentin, 2010; Moody et al., 2018; Vrhovec & Mihelič, 2021) although it was originally developed to explain the effects of fear appeals on health attitudes and behavior (Floyd et al., 2000; Rogers, 1975). PMT is organized along two cognitive processes, namely, threat appraisal and coping appraisal (Boss et al., 2015; Floyd et al., 2000; Mousavi et al., 2020; Vrhovec & Mihelič, 2021). Threat appraisal consists of appraisal of an individual's vulnerability to a threat and severity of the consequences if a threat realizes (Y. Choi, 2019; Floyd et al., 2000). Perceived threat has been established as a separate construct mediating the associations between perceived vulnerability and severity, and protection motivation in later studies (Fujs et al., 2019; Liang & Xue, 2010; Vrhovec & Mihelič, 2021). Coping appraisal includes locus of control which may be used to predict why people assume responsibility for their own security and employ protective measures (Jansen & van Schaik, 2018). Protection motivation in the context of cybersecurity may be also related to privacy concern albeit the published results have been mixed (Benamati et al., 2017; Fujs et al., 2019).

Figure 1. Research model



Privacy is defined as a right of people to voluntarily decide under what conditions and to what extent they will expose themselves, their attitude and their behavior to others, and has been a sensitive issue even before the invention of computers (Dinev et al., 2008; K.-W. Wu et al., 2012). Technological development and high adoption of internet services, such as social media, appear to have led to a loss of personal privacy (Dinev et al., 2008). On one hand, social media users leave many digital footprints that allow automatic recognition of their behavior and enable invasions of their privacy (Lutz et al., 2020; K.-W. Wu et al., 2012). On the other hand, social media users are willing to risk their privacy for enjoying the benefits of social media, such as developing relationships and pleasures of using different services offered on social media (Horne & Przepiorka, 2019; Krasnova et al., 2010; Lutz et al., 2020; Tsay-Vogel et al., 2018). This phenomena is also known as the privacy paradox and is commonly explained by the privacy calculus theory (Lutz et al., 2018; Marwick & Hargittai, 2019; Obar & Oeldorf-Hirsch, 2020; Vassallo, 2019). Privacy concern may have different dimensions, such as collection, secondary usage, errors, improper access, control and awareness (Hong & Thong, 2013). Each dimension deals with a different aspect of concerns that people may have regarding the ability and willingness of online entities to protect them against unwanted intrusions into their privacy (H. Xu & Gupta, 2009). In this paper, we focus on privacy concern related to the collection of data as it precedes its other dimensions.

Based on the above, we develop the following hypotheses:

H1: Perceived threat of intrusions into accounts on social media is positively associated with motivation to self-protect on social media.
H2: Locus of control for self-protecting on social media is positively associated with motivation to self-protect on social media.
H3: Concern regarding privacy on social media is positively associated with motivation to self-protect on social media.

The emergence of the internet enabled governments to reach out to citizens and exchange information with them through various platforms, such as official web pages, e-mails, media and most recently social media (de Arruda et al., 2020). However, governments may seek a deeper insight into citizens online activities for both justified (e.g., crime investigations, anti-terrorism operations) and unjustified (e.g., mass surveillance to tackle political dissent) reasons (Bieniasz & Szczypiorski, 2019; Diehl et al., 2016; Lenarčič, 2020; Završnik, 2019). Paradoxically, government surveillance may be necessary for ensuring trust in a society of individuals who value privacy (Dinev et al., 2008).

Fear of government intrusions is an emotion that is fueled by the internet users' perceived threat of government intrusions into their privacy, and may affect their behavior online (Juola, 2020; S. Wu, 2020). In this study, we assume that fear of government intrusions feeds into the perceived threat of general intrusions into social media accounts since governments are among the more capable adversary actors in the cyberspace. We also assume that privacy concern is a materialization of such fear. Thus, we suggest the following hypotheses:

H4a: Fear of government intrusions is positively associated with perceived threat of intrusions into accounts on social media.
H4b: Fear of government intrusions is positively associated with concern regarding privacy on social media.

Trust is an important component of online interactions due to their inherent risks and dependency on various service providers (e.g., ISP, social media provider) (Martínez et al., 2020; Mou et al., 2016; Shin, 2010). Trust may be defined in various ways and may be directed towards different entities, such as technology, service providers, and the government (Chen et al., 2015; McKnight et al., 2002a). In this paper, we define trust as the willingness of an individual to be vulnerable to the actions of the trusted entity based on the expectation that the trusted entity will perform a particular action important to the individual irrespective of his or her ability to monitor or control the trusted entity (McKnight et al., 2002a, 2002b; Shin, 2010).

Although the relation between trust and various types of online behavior in different contexts were studied in the past (Martínez et al., 2020; Menard & Bott, 2020; Wang et al., 2020), it is unclear how trust in actors related to government surveillance are related to perceived threat of social media users or their privacy concern. In this study, we assume that trust in government, which reflects the general situation in politics, government and its services, lowers perceived threat and privacy concern of social media users. Since government surveillance may be done through ISP, we posit the following hypotheses:

H5a: Trust in government is negatively associated with perceived threat of intrusions into accounts on social media.
H5b: Trust in government is negatively associated with concern regarding privacy on social media.
H6a: Trust in internet service provider is negatively associated with perceived threat of intrusions into accounts on social media.
H6b: Trust in internet service provider is negatively associated with concern regarding privacy on social media.

Studies found a significant association between privacy concern and trusting beliefs (Lutz et al., 2018; Taddei & Contena, 2013; Van Dyke et al., 2007). In this study we however posit that trust in social media provider moderates the relation between privacy concern and protection motivation which may offer a new piece of the privacy paradox puzzle. Therefore, we propose the following hypothesis:

H7: Trust in social media provider strengthens the positive association between concern regarding privacy on social media and motivation to self-protect on social media.

METHOD

Design

A cross-sectional survey research design was used to explore the associations between perceptions about government and social media providers, and protection motivation on social media.

Ethical Considerations

This study did not require an approval from the Institutional Review Board according to the legislation of the Republic of Slovenia and internal acts of the University of Maribor. Nevertheless, ethical standards were strictly followed throughout the study. Respondents participated in the study voluntarily and anonymously. No personally identifiable information was collected. Respondents were presented with the aim and broad overview of the study before taking the survey. They also provided their informed consent before taking the survey. The study did not involve misleading of participants in any way, and it did not inflict any harm (e.g., psychological harm). Participants did not receive any incentives for taking part in the survey.

Measures

Theoretical constructs were defined and operationalized as presented in Table 1. All measured constructs were reflective, and their items were either previously validated or adapted from previously validated items. Items for *fear of government intrusions* were adapted from (Osman et al., 1994). Items for *trust in government*, *trust in internet service provider* and *trust in social media provider*

Table 1. Definitions of theoretical constructs

Theoretical construct	Operational definition
Fear of government intrusions	The extent of fear regarding government intrusions into privacy.
Trust in government	The degree of trust in government of the current country of residence.
Trust in internet service provider	The degree of trust in internet service provider.
Trust in social media provider	The degree of trust in social media provider.
Perceived threat	The degree to which intrusions into accounts on social media threaten their users.
Privacy concern	The extent of concern regarding privacy on social media.
Locus of control	The extent to which individuals take responsibility for self-protecting on social media themselves.
Protection motivation	The degree of motivation to self-protect on social media.

were adapted from (McKnight et al., 2002b). Items for *locus of control* were adapted from (Jansen & van Schaik, 2018). Items for *perceived threat*, *privacy concern*, and *protection motivation* were taken from (Fujs et al., 2019). All items were measured by using a 5-point Likert scale from 1 "strongly disagree" to 5 "strongly agree".

The survey was distributed in Slovenian which was the primary language of all respondents in our study. Adapted items (i.e., fear of government intrusions, trust in government, trust in internet service provider, trust in social media provider, and locus of control) were developed by following a predefined protocol as follows. The questionnaire was first developed in English and then translated into Slovenian by two translators independently. The translators developed the Slovenian questionnaire through consensus. The Slovenian questionnaire has been pre-tested by 3 independent respondents who provided feedback on its clarity. Based on the received feedback, the Slovenian questionnaire was reviewed to remove any ambiguity. Items were reworded, added, and deleted in the pre-test. To ensure the consistency between the Slovenian and English questionnaire, the Slovenian questionnaire was translated back to English. No significant differences in the meaning between the original items in English and back-translations were noticed. The English questionnaire was however reviewed to update the items and to remove any ambiguity based on the back-translation.

Sample and Data Collection

We conducted an online survey among students at a Slovenian university. On one hand, students represent an important portion of internet users that are highly connected, have a tendency to engage in risky behaviors online, and are often unaware of the consequences of not using security measures (Aurigemma et al., 2019; Cai et al., 2017; Mensch & Wilkie, 2019). On the other hand, students are one of the key target groups for government surveillance in countries that deem them as a potential risk to the regime. Governments can influence internet service providers in their countries, and may try to influence social media providers even though their leverage may be much lower when they are headquartered in another country. Based on the above and since the vast majority of students in Slovenia have at least one social media account, we deemed them as appropriate for our study since we wanted to study protection motivation of a key group of social media users in a country with medium surveillance concern (Fujs & Vrhovec, 2019).

The population of the web survey consisted of 988 students with university-provided e-mails. A total of 289 respondents completed the survey providing for a response rate of 29.3 percent. After excluding poorly completed responses, we were left with *N*=276 useful responses for further analysis. The data were gathered from October 2018 to January 2019. Table 2 provides an overview of the sample demographics.

Table 2. Sample and population demographic characteristics

	Sample		Population
Gender			
Male	91	33.0%	44.3%
Female	174	63.0%	55.7%
N/A	11	4.0%	
Age			
18-24	192	69.6%	70.0%
25-29	41	14.9%	15.7%
30-34	12	4.3%	4.2%
35-39	11	4.0%	3.5%
40+	9	3.3%	6.6%
N/A	11	4.0%	
Employment status			
Student	215	77.9%	-
Employed	41	14.9%	-
Unemployed	8	2.9%	-
N/A	12	4.3%	
Formal education			
High school or less	144	52.2%	74.6%
Bachelor’s degree	91	33.0%	23.9%
Master’s degree	25	9.1%	1.5%
Doctoral degree	4	1.4%	0.1%
N/A	12	4.3%	

Sample demographics are comparable to the population in terms of age groups except for the age group 40+ which seems to be slightly underrepresented. There is a slightly higher proportion of female respondents in the sample (63.0%) than in the population (55.7%). In the sample, the proportion of undergraduate and graduate levels of formal education are more represented than in the population.

The invitations were sent to university-provided emails of all students. Since these email addresses are frequently used throughout the studies and all students had the possibility to participate in the study, we deemed this as a random sample despite these differences between the sample and population demographics.

Data Analysis

Partial least squares structural equation modeling (PLS-SEM) was used to test the proposed research model. PLS-SEM is particularly suitable for exploratory research where theory is less developed, and for testing continuous moderators (Hair et al., 2017) as is the case in our study. The collected data were processed with IBM SPSS Statistics 27 (descriptive statistics only), R version 3.6.3, and SEMinR version 2.2.1.

There were 1.7 percent missing values which were imputed with medians before data analysis with PLS-SEM. The survey instrument was first validated with a confirmatory factor analysis. Construct items were tested for their reliability, convergent validity and discriminant validity. Reliability was tested by calculating composite reliability (*CR*). Values above 0.60 are acceptable and values above

0.70 are recommended (H.-C. Lin & Chang, 2018). Convergent validity was determined examining average variance extracted (*AVE*). Values above 0.50 are recommended however values below this threshold may be acceptable if *CR* is adequate (Hu & Bentler, 1999; H.-C. Lin & Chang, 2018). Discriminant validity was determined by heterotrait-monotrait ratio of correlations (HTMT) analysis.

A structural model was then constructed to test hypotheses H1, H2, H3, H4a, H4b, H5a, H5b, H6a, and H6b. The moderating effect of trust in social media provider on the association between privacy concern and protection motivation (H7) was investigated by constructing a second structural model (namely, interaction analysis structural model) by following a product indicator approach in a fully latent structural model. The new construct was formed as the product of indicators of privacy concern and trust in social media provider. Both structural models were estimated with bootstrap resampling with 5,000 replications.

RESULTS

Instrument validation

A measurement model was developed to validate the survey instrument. Table 3 presents *CR*, *AVE* and HTMT analysis which are relevant for determining the validity and reliability of the survey instrument. First, *CR* ranged from 0.781 to 0.921 thus exceeding the commonly accepted threshold 0.70. This demonstrates adequate reliability of all constructs. Next, *AVE* ranged from 0.550 to 0.795. Values above the 0.50 threshold are generally considered as adequate therefore indicating adequate convergent validity. Additionally, factor loadings (see Table 4) except for TiG2, TiISP2, TiSMP3, PC1, PC3, and LoC3 were above the 0.70. Since all other indicators suggested adequate convergent validity, we did not consider this as a serious issue. Finally, HTMT ratios of correlations were all below the conservative 0.85 threshold thus indicating adequate discriminant validity of the survey instrument.

To reduce the likelihood of social desirability bias, we informed the respondents that participation in the research is voluntary and anonymous while the data will be used exclusively for research purposes. To test for the presence of common method bias, Harman's single factor test was conducted. A single factor accounted for 15.3 percent of the variance which is well below the threshold of 50 percent indicating the common method bias was not a major issue in our study (Pesämaa et al., 2021; Podsakoff et al., 2003).

Structural Model

A structural model was first developed to test the hypothesized associations. Figure 2 presents standardized path coefficients, their *p*-values, effect sizes f^2, and adjusted R^2. Constructs in the model explain a meaningful share of variance of all predicted constructs (i.e., perceived threat, privacy concern and protection motivation).

Table 3. Validity and reliability of the survey instrument. Composite reliability (CR), average variance extracted (AVE), and heterotrait-monotrait ratio of correlations (HTMT) analysis

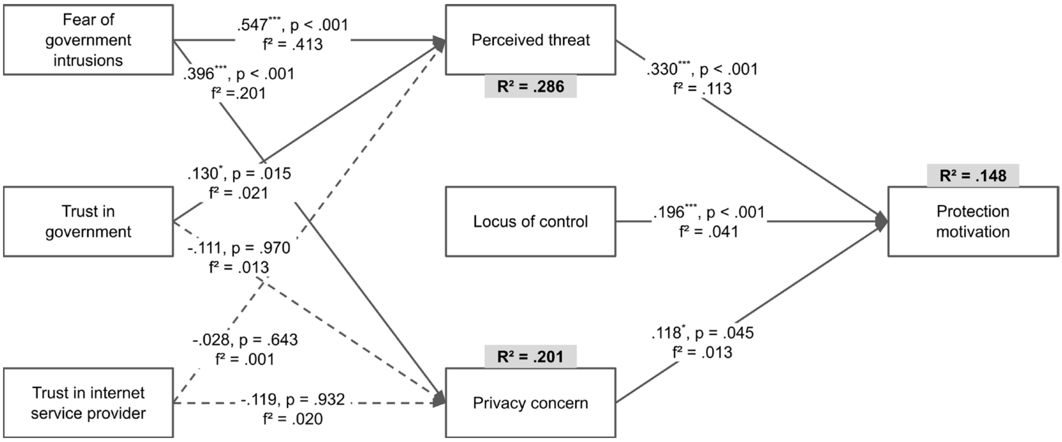
Construct	CR	AVE	1	2	3	4	5	6	7
1. Fear of government intrusions	.893	.737							
2. Trust in government	.874	.703	.189						
3. Trust in internet service provider	.789	.574	.100	.393					
4. Trust in social media provider	.798	.578	.105	.305	.826				
5. Perceived threat	.825	.613	.688	.063	.099	.152			
6. Privacy concern	.781	.550	.509	.253	.214	.287	.286		
7. Locus of control	.812	.601	.138	.120	.289	.308	.242	.166	
8. Protection motivation	.921	.795	.249	.043	.100	.060	.412	.256	.178

Table 4. Questionnaire items

Construct	Loading	Prompt/Item
Fear of government intrusions		Mark your agreement with statements about the government of the country where you currently reside:
	.799	FoGI1. Government intrusions into my privacy are terrifying.
	.922	FoGI2. I am afraid of government intrusions into my privacy.
	.850	FoGI3. The government might be seriously invading my privacy.
Trust in government		Mark your agreement with statements about the government of the country where you currently reside:
	.866	TiG1. I believe that the government would act in my best interest.
	.670	TiG2. The government is interested in my well-being not just its own.
	.954	TiG3. I would characterize the government as honest.
Trust in internet service provider		Mark your agreement with statements about your internet service provider:
	.952	TiISP1. I believe that the internet service provider would act in my best interest.
	.459	TiISP2. The internet service provider is interested in my well-being not just its own.
	.777	TiISP3. I would characterize the internet service provider as honest.
Trust in social media provider		Mark your agreement with statements about providers of social networks on which you have accounts (e.g., Facebook, Twitter, Instagram, Snapchat, WhatsApp, Telegram, Tinder):
	.926	TiSMP1. I believe that social network providers would act in my best interest.
	.756	TiSMP2. Social network providers are interested in my well-being not just their own.
	.552	TiSMP3. I would characterize social network providers as honest.
Perceived threat		Mark your agreement with statements about potential intrusions into one of your social network accounts:
	.870	PT1. I feel threatened by intrusions.
	.732	PT2. Intrusions threaten my accounts.
	.740	PT3. It would be dreadful if there would be an intrusion into one of my accounts.
Privacy concern		Mark your agreement with statements about your personal data on social networks (e.g., Facebook, Twitter, Instagram, Snapchat, WhatsApp, Telegram, Tinder):
	.645	PC1. It highly bothers me when social networks ask me about my personal data.
	.911	PC2. I always think twice before submitting my personal data to social networks.
	.635	PC3. I am very concerned that social networks collect too much personal data about me.
Locus of control		Mark your agreement with statements about control over your social network accounts:
	.832	LoC1. Keeping my accounts safe is within my control.
	.914	LoC2. I believe that it is within my control to protect myself against hacking into my accounts.
	.525	LoC3. The primary responsibility for protecting my accounts against hacking belongs to me.
Protection motivation		Mark your agreement with statements about implementing recommended security measures on social networks (e.g., periodical password changes, use of strong passwords, paying attention to login alerts):
	.865	PM1. I intend to implement recommended security measures regularly.
	.922	PM2. I predict that I will implement recommended security measures in the near future.
	.886	PM3. I plan to implement recommended security measures.

Figure 2. Structural model

*Notes: * $p < 0.05$, *** $p < 0.001$*


Fear of government intrusions
$.547^{***}$, $p < .001$ $f^2 = .413$
$.396^{***}$, $p < .001$ $f^2 = .201$
Perceived threat
$R^2 = .286$
$.330^{***}$, $p < .001$ $f^2 = .113$
$.130^{*}$, $p = .015$ $f^2 = .021$
Trust in government
$-.111$, $p = .970$ $f^2 = .013$
Locus of control
$.196^{***}$, $p < .001$ $f^2 = .041$
$R^2 = .148$
Protection motivation
$-.028$, $p = .643$ $f^2 = .001$
$R^2 = .201$
$.118^{*}$, $p = .045$ $f^2 = .013$
Trust in internet service provider
$-.119$, $p = .932$ $f^2 = .020$
Privacy concern

The results support hypotheses H1 and H2 ($p < .001$), and H3 ($p = .045$). Nevertheless, all three associations have small effect sizes (i.e., $f^2 < .15$). The association between perceived threat and protection motivation has largest effect of the three ($f^2 = .113$), indicating that its the strongest among them. There is also support for hypotheses H4a and H4b ($p < .001$) with large (i.e., $f^2 > .30$) and medium effect sizes, respectively. The structural model also shows some counter-support for hypothesis H5a ($p = .015$) albeit the effect size is small. There is however no support for hypotheses H5b, H6a and H6b ($p > .1$).

A second structural model was constructed to test hypothesis H7 as presented in Figure 3. The results indicate support for the moderating role of trust in social media provider ($p = .016$) even though the effect size is small. The noticeably higher R^2 for protection motivation further supports hypothesis H7. Additionally, these results offer also support for hypotheses H1, H2, and H3 ($p < .001$).

To gain further insights into the moderating role of trust in social media provider, we performed a simple slope analysis shown in Figure 4. The simple slope analysis appears to suggest that privacy concern is not associated with protection motivation if trust in social media provider is low as the line is almost horizontal. The association however seems quite strong if trust in social media provider is high.

The summary of hypotheses testing is presented in Table 5.

DISCUSSION

The purpose of this study was to explore the relations between perceptions about government (i.e., fear of government intrusions, trust in government and trust in ISP) and social media providers (i.e., trust in social media provider), and protection motivation of users on social media. Even though we report on an exploratory study, the results suggest several theoretical and practical implications as discussed in the following subsections.

Theoretical Implications

This study has several theoretical implications. First, this is one of the first studies exploring the associations between fear of government intrusions into privacy, trusting beliefs towards government and ISP, and privacy concern of social media users. These insights contribute to the privacy literature. The absence of significant associations between trust in government and trust in ISP suggest that trusting beliefs do not have a major role in shaping privacy concern of social media users. Nevertheless, a

Figure 3. Interaction analysis structural model

*Notes: * p < 0.05, *** p < 0.001*

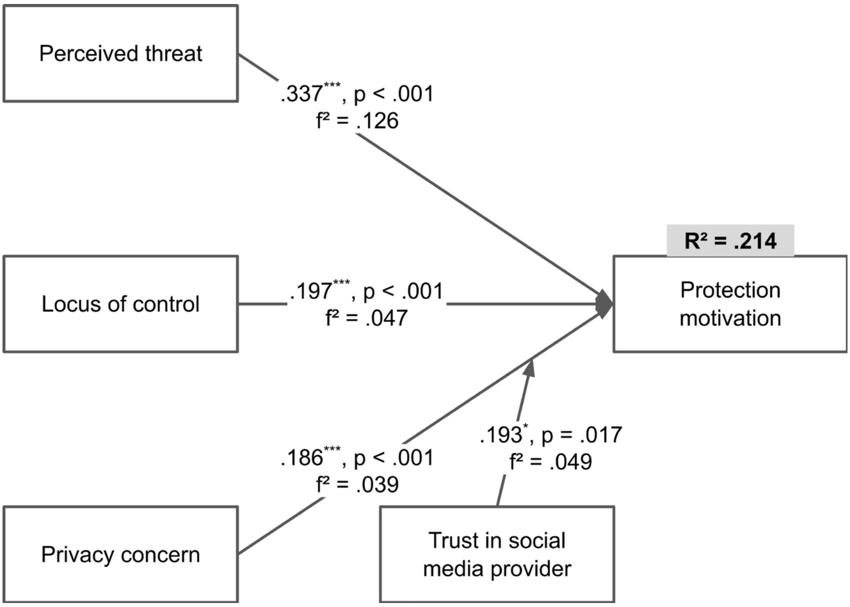
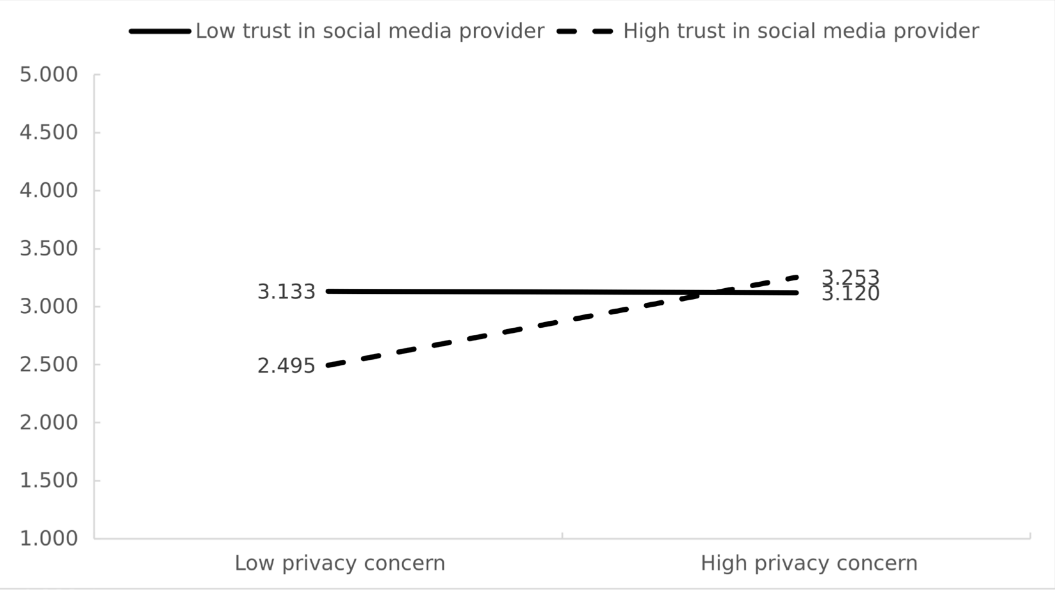


Figure 4. Interaction between trust in social media provider and privacy concern. Higher scores indicate higher protection motivation



significant association between fear of government intrusions and privacy concern indicates that privacy concern is indeed related to perceptions about government. Social media users who fear government intrusions into their privacy tend to have higher privacy concern. Albeit governments may be more limited in influencing social media providers, they may still be perceived by social media users as a key actor affecting their privacy, e.g., due to national security reasons or to tackle political dissent.

Table 5. Hypotheses testing summary

Hypothesis	Evidence	Conclusion
H1: Perceived threat of intrusions into accounts on social media is positively associated with motivation to self-protect on social media.	Significant positive paths in both structural models, small effect size	Supported
H2: Locus of control for self-protecting on social media is positively associated with motivation to self-protect on social media.	Significant positive paths in both structural models, small effect size	Supported
H3: Concern regarding privacy on social media is positively associated with motivation to self-protect on social media.	Significant positive paths in both structural models, small effect size	Supported
H4a: Fear of government intrusions is positively associated with perceived threat of intrusions into accounts on social media.	Significant positive path, large effect size	Supported
H4b: Fear of government intrusions is positively associated with concern regarding privacy on social media.	Significant positive path, medium effect size	Supported
H5a: Trust in government is negatively associated with perceived threat of intrusions into accounts on social media.	Significant positive path, small effect size	Rejected
H5b: Trust in government is negatively associated with concern regarding privacy on social media.	Non-significant path	Not supported
H6a: Trust in internet service provider is negatively associated with perceived threat of intrusions into accounts on social media.	Non-significant path	Not supported
H6b: Trust in internet service provider is negatively associated with concern regarding privacy on social media.	Non-significant path	Not supported
H7: Trust in social media provider strengthens the positive association between concern regarding privacy on social media and motivation to self-protect on social media.	Significant strengthening interaction	Supported

Fear of government intrusions may depend both on the personal characteristics of social media users, and the compatibility of social media users with the government of the country in which they reside. These results also imply that privacy concern of social media users may depend on the country in which they reside as fear of government intrusions varies around the globe (Fujs & Vrhovec, 2019). The results of our study may also suggest, for example, that minorities, migrants and other non-native residents, and temporary residents (e.g., tourists and business travelers) may have differing privacy concern from the native residents of a specific country. On one hand, this could be due to the differences in their compatibility with the government or detachment from the governmental institution in a foreign country. On the other hand, differences may be due to cultural differences of non-native residents. To further explore these propositions, future research should be conducted globally in various countries around the world.

Second, this is one of the first studies to explore the relations between perceptions about government and threat appraisal according to the protection motivation theory (Floyd et al., 2000; Liang & Xue, 2010; Vrhovec & Mihelič, 2021). The results indicate that fear of government intrusions is strongly associated with perceived threat with a large effect size. Respondents may consider the government as either an important source of potential intrusions or as a key facilitator of intrusions by other threat actors. Even if a government cannot or does not want to threaten social media accounts directly, it may either seek experts for specific projects or support other actors doing so. We should note that we do not assume that governments, especially democratically elected, are invading the privacy of social media users. It is about the perceptions of social media users, no matter how justified.

The positive association between trust in government and perceived threat seems puzzling. It is counter-intuitive that the more social media users trust in government the more they perceive their social media accounts to be threatened. A simple explanation would be a false positive (i.e., type I error). Future studies would be needed to determine if this is the case. There are however alternative explanations possible as perceived threat is not directly linked to the government. There are several actors in the cyberspace that can threaten social media accounts (e.g., individuals who are known to social media users, cybercriminals, state-sponsored actors, hackers and hacktivists). It is therefore possible that people who tend to trust faster (as a personal trait) also feel that their social media accounts are more threatened, or even feel more threatened online in general. A counter-argument could be that trust in ISP was not significantly associated with perceived threat. Albeit this could be a valid argument, it seems that the respondents did not consider ISP as a relevant actor at all (no significant associations). From the user perspective, ISP plays a passive role (i.e., providing the underlying infrastructure and services for accessing the internet) that may seem irrelevant from the security and privacy perspective. In this case, the above argument would be void.

The results of our study therefore show strong support for including fear of government intrusions in research models including threat appraisal of social media users. The absence of a credible explanation for a positive association between trust in government and perceived threat however requires further investigation for a stronger contribution to the literature. This study therefore contributes to the literature on protection motivation on social media. Future studies may additionally seek to provide further insight into the role of fear of government intrusions in threat appraisal online - in general, not only in the context of social media.

Third, this study advances our understanding of the association between privacy concern and protection motivation. Published literature indicates support that privacy concern associates with protection motivation, sharing information and other privacy-protecting behavior (Fujs et al., 2019; Krasnova et al., 2010; Lutz et al., 2020; Tsay-Vogel et al., 2018) albeit not always (Brown, 2020; Nam, 2017). The results of our study may be able to provide some insights into the reasons why. Contrary to existing studies that consider privacy concern as a mediator between trust in social media provider and privacy-protecting behavior (e.g., (Krasnova et al., 2010)) or trust in social media provider as an outcome of privacy concern, our study shows that trust in social media provider is a moderator between privacy concern and privacy-protecting behavior, specifically protection motivation. The results suggest that privacy concern is associated with protection motivation only when trust in social media provider is high. When trust in social media provider is low, privacy concern may not be associated with protection motivation at all. It may be because of the futility of implementing the recommended security measures if social media provider is the problematic actor threatening a social media account who can circumvent them anyway. This contributes to the literature on both privacy and protection motivation on social media. Future studies may thus consider the moderating role of online service providers when studying the relation between privacy concern and protection motivation.

Practical Implications

This study also has some practical implications for different stakeholders. First, our study suggests that governments may have conflicting objectives in the context of social media. Arguably, governments in democratic countries aim to promote good ideas and avoid bad ones. If the good idea is to improve social media users' security on social media by motivating them to protect themselves, the results of our study indicate that increasing government fear of intrusions is the most effective way to do so. However, this can hardly be considered as a "good" idea as it would erode the sense of security and privacy online which may be also counter to the governments' objective of establishing a trustworthy digital environment, such as the Digital Single Market in the European Union.

Governments also need to consider the balance between privacy and security. The need to do this appears to be continuously changing according to the situation. For example, several countries are currently striving to change surveillance legislation in response to the rise in terrorism in recent years (Trüdinger & Steckermeier, 2017). It may be acceptable to justify government intrusions into privacy of residents during periods of a heightened need to provide security.

Second, the results of our study suggest that social media providers do not need to earn trust from social media users if they want to motivate them to protect themselves. The results suggest that social media users with low trust in social media provider are quite well-motivated to protect themselves. This surprisingly implies that privacy-related scandals, such as Facebook – Cambridge Analytica, may have actually contributed positively to the overall protection motivation of social media users. This may be counter intuitive as protective measures cannot protect against a social media provider that is providing them. Social media providers however do need to further motivate social media users that trust them by other means, such as affecting their threat appraisal (e.g., with awareness interventions), since it would not be in their interest to lower social media users' trusting beliefs towards the provider.

Limitations and Future Research

This paper reports on an exploratory study and several limitations need to be considered when interpreting its results. First, the study was conducted in a single country. Since fear of government intrusions and trust in government may be dependent on the country (e.g., the dichotomy between democratic and authoritarian regimes), the findings may not be applicable across different countries and periods. Future work including a variety of countries would be highly beneficial to address this limitation although it may be hard to include countries with highly repressive regimes. Second, the population were students at a single university. Albeit the sample was fairly random, generalizing to all students (e.g., from other universities, in different cultural contexts, different countries) should be done with caution. Future studies may broaden the richness of societal and cultural contexts which would provide valuable insights into the topic. Third, the findings of this study may not be generalized to all social media users as all respondents were students. Although students represent an important portion of social media users, future studies including other social media users would improve the ecological validity of this study. Future studies may also research the impact of cultural characteristics of social media usage. This study does not focus on a specific type of social media. Social media are not uniform, have different characteristics and defining attributes (e.g., posting photos on Instagram, direct messages on WhatsApp, short news-like tweets on Twitter), and attract different profiles of users. Research focusing on specific social media and potentially comparing different insights may be beneficial, too.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to the respondents who took their time to participate in our survey. We would also like to thank the anonymous reviewers for their insightful and constructive comments.

CONFLICT OF INTEREST

The authors of this publication declare there is no conflict of interest.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Aurigemma, S., Mattson, T., & Leonard, L. (2019). Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transactions on Replication Research*, *5*, 1–21. doi:10.17705/1atrr.00035

Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, (pp. 258–265). IEE/ACM. doi:10.1109/ASONAM.2018.8508646

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents – Privacy Concerns – Outcomes model. *Journal of Information Science*, *43*(5), 583–600. doi:10.1177/0165551516653590

Bieniasz, J., & Szczypiorski, K. (2019). Methods for Information Hiding in Open Social Networks. *Journal of Universal Computer Science*, *25*(2), 74–97. doi:10.3217/jucs-025-02-0074

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber Attacks, Contributing Factors, and Tackling Strategies. *International Journal of Cyber Behavior, Psychology and Learning*, *7*(4), 68–82. doi:10.4018/IJCBPL.2017100106

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. *Management Information Systems Quarterly*, *39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

Brown, A. J. (2020). "Should I Stay or Should I Leave?": Exploring (Dis)continued Facebook Use After the Cambridge Analytica Scandal. *Social Media + Society*, *6*(1), 205630512091388. doi:10.1177/2056305120913884

Cai, Z., Fan, X., & Du, J. (2017). Gender and attitudes toward technology use: A meta-analysis. *Computers & Education*, *105*, 1–13. doi:10.1016/j.compedu.2016.11.003

Chen, J. V., Jubilado, R. J. M., Capistrano, E. P. S., & Yen, D. C. (2015). Factors affecting online tax filing – An application of the IS Success Model and trust theory. *Computers in Human Behavior*, *43*, 251–262. doi:10.1016/j.chb.2014.11.017

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. doi:10.1016/j.chb.2017.12.001

Choi, Y. (2019). Organizational Control Policy, Information Security Deviance, and Moderating Effect of Power Distance Orientation. *International Journal of Cyber Behavior, Psychology and Learning*, *9*(3), 48–60. doi:10.4018/IJCBPL.2019070104

Comparitech. (2021). *Test if a site is blocked in China*. Comparitech.Com. https://www.comparitech.com/privacy-security-tools/blockedinchina/

de Arruda, G. D., Roman, N. T., & Monteiro, A. M. (2020). Analysing bias in political news. *Journal of Universal Computer Science*, *26*(2), 173–199. doi:10.3897/jucs.2020.011

Diehl, T., Weeks, B. E., & Gil de Zúñiga, H. (2016). Political persuasion on social media: Tracing direct and indirect effects of news use and social interaction. *New Media & Society*, *18*(9), 1875–1895. doi:10.1177/1461444815616224

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233. doi:10.1016/j.jsis.2007.09.002

Erdbrink, T. (2013). Iran Bars Social Media Again After a Day. *The New York Times*. https://www.nytimes.com/2013/09/18/world/middleeast/facebook-and-twitter-blocked-again-in-iran-after-respite.html

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. doi:10.1111/j.1559-1816.2000.tb02323.x

Fujs, D., Mihelič, A., Vrhovec, S., & Mihelič, A. (2019). Social Network Self-Protection Model:What Motivates Users to Self-Protect? *Journal of Cyber Security and Mobility*, *8*(4), 467–492. doi:10.13052/jcsm2245-1439.844

Fujs, D., & Vrhovec, S. (2019). Cyber landscape of trust, fear and surveillance concerns : How Slovenians around the globe perceive the cyberspace. *Varstvoslovje*, *21*(4), 333–345.

Fujs, D., Vrhovec, S., & Mihelič, A. (2018). What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats. *Proceedings of the Central European Cybersecurity Conference 2018 on - CECC 2018*, (pp. 1–6). ACM. doi:10.1145/3277570.3277581

Hair, J. F. J., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107. doi:10.1504/IJMDA.2017.087624

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *Management Information Systems Quarterly*, *37*(1), 275–298. doi:10.25300/MISQ/2013/37.1.12

Horne, C., & Przepiorka, W. (2019). Technology use and norm change in online privacy: Experimental evidence from vignette studies. *Information Communication and Society*, 1–17. doi:10.1080/1369118X.2019.1684542

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, *6*(1), 1–55. doi:10.1080/10705519909540118

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59. doi:10.1109/MC.2018.3191268

Jansen, J., & van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior*, *87*, 371–383. doi:10.1016/j.chb.2018.05.010

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *Management Information Systems Quarterly*, *34*(3), 549. doi:10.2307/25750691

Juola, P. (2020). Autorship Studies and the Dark Side of Social Media Analytics. *Journal of Universal Computer Science*, *26*(1), 156–170. doi:10.3897/jucs.2020.009

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

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 109–125. doi:10.1057/jit.2010.6

Lee, O.-J., Kim, Y., Nguyen, H. L., & Jung, J. E. (2018). Multi-scaled spatial analytics on discovering latent social events for smart urban services. *Journal of Universal Computer Science*, *24*(3), 322–337.

Lenarčič, B. (2020). Migracijski proces v omrežni družbi. *Dve Domovini / Two Homelands, 51*(1), 167–183. 10.3986/dd.2020.1.10

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. doi:10.17705/1jais.00232

Lin, H.-C., & Chang, C.-M. (2018). What motivates health information exchange in social media? The roles of the social cognitive theory and perceived interactivity. *Information & Management*, *55*(6), 771–780. doi:10.1016/j.im.2018.03.006

Lin, S.-W., & Liu, Y.-C. (2012). The effects of motivations, trust, and privacy concern in social networking. *Service Business*, *6*(4), 411–424. doi:10.1007/s11628-012-0158-6

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information Communication and Society*, *21*(10), 1472–1492. doi:10.1080/1369118X.2017.1339726

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, *22*(7), 1168–1187. doi:10.1177/1461444820912544

Martínez, P., Herrero, Á., & García-de los Salmones, M. del M. (2020). Determinants of eWOM on hospitality CSR issues. In Facebook we trust? *Journal of Sustainable Tourism*, *28*(10), 1479–1497. doi:10.1080/09669582.2020.1742133

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information Communication and Society*, *22*(12), 1697–1713. doi:10.1080/1369118X.2018.1450432

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002a). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. doi:10.1287/isre.13.3.334.81

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002b). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *The Journal of Strategic Information Systems*, *11*(3–4), 297–323. doi:10.1016/S0963-8687(02)00020-3

Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, *95*, 101856. doi:10.1016/j.cose.2020.101856

Mensch, S. E., & Wilkie, L. (2019). Smart Phone Security Practices. *International Journal of Cyber Behavior, Psychology and Learning*, *9*(3), 1–14. doi:10.4018/IJCBPL.2019070101

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *Management Information Systems Quarterly*, *42*(1), 285–311. doi:10.25300/MISQ/2018/13853

Mosteller, J., & Poddar, A. (2017). To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviors. *Journal of Interactive Marketing*, *39*, 27–38. doi:10.1016/j.intmar.2017.02.003

Mou, Y., Wu, K., & Atkin, D. (2016). Understanding the use of circumvention tools to bypass online censorship. *New Media & Society*, *18*(5), 837–856. doi:10.1177/1461444814548994

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*, 113323. doi:10.1016/j.dss.2020.113323

Nam, T. (2017). Does ideology matter for surveillance concerns? *Telematics and Informatics*, *34*(8), 1572–1585. doi:10.1016/j.tele.2017.07.004

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society*, *23*(1), 128–147. doi:10.1080/1369118X.2018.1486870

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., & Troutman, J. A. (1994). The Pain Anxiety Symptoms Scale: Psychometric properties in a community sample. *Journal of Behavioral Medicine*, *17*(5), 511–522. doi:10.1007/BF01857923 PMID:7877159

Pesämaa, O., Zwikael, O., Hair, J. F. Jr, & Huemann, M. (2021). Publishing quantitative papers with rigor and transparency. *International Journal of Project Management*, *39*(3), 217–222. doi:10.1016/j.ijproman.2021.03.001

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879 PMID:14516251

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803 PMID:28136248

Shin, D.-H. (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

Sivasangari, V., Mohan, A. K., Suthendran, K., & Sethumadhavan, M. (2018). Isolating Rumors Using Sentiment Analysis. *Journal of Cyber Security and Mobility*, *7*(1), 181–200. doi: doi:10.13052/jcsm2245-1439.7113

Specht, D., & Ros-Tonen, M. A. F. (2017). Gold, power, protest: Digital and social media and protests against large-scale mining projects in Colombia. *New Media & Society*, *19*(12), 1907–1926. doi:10.1177/1461444816644567

Steinebach, M., Gotkowski, K., & Liu, H. (2020). Fake news detection by image montage recognition. *Journal of Cyber Security and Mobility*, *9*(2), 175–202. doi:10.13052/jcsm2245-1439.921

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. doi:10.1016/j.chb.2012.11.022

Talmadge, E. (2016). *North Korea blocks Facebook, Twitter and YouTube*. Globalnews.Ca. https://globalnews.ca/news/2616449/north-korea-blacks-facebook-twitter-and-youtube/

Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, *34*(3), 421–433. doi:10.1016/j.giq.2017.07.003

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141–161. doi:10.1177/1461444816660731

Tundis, A., Böck, L., Stanilescu, V., & Mühlhäuser, M. (2020). Experiencing the detection of radicalized criminals on facebook social network and data-related issues. *Journal of Cyber Security and Mobility*, *9*(2), 203–236. doi:10.13052/jcsm2245-1439.922

Uldam, J. (2016). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society*, *18*(2), 201–219. doi:10.1177/1461444814541526

Van Dyke, T., Midha, V., & Nemati, H. (2007). The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce. *Electronic Markets*, *17*(1), 68–81. doi:10.1080/10196780601136997

Vassallo, M. (2019). The Privacy Paradox in the Big Data Era? No Thanks, We Are the E-People. *International Journal of Cyber Behavior, Psychology and Learning*, *9*(3), 32–47. doi:10.4018/IJCBPL.2019070103

Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, 102309. doi:10.1016/j.cose.2021.102309

Wang, Y., Asaad, Y., & Filieri, R. (2020). What Makes Hosts Trust Airbnb? Antecedents of Hosts' Trust toward Airbnb and Its Impact on Continuance Intention. *Journal of Travel Research*, *59*(4), 686–703. doi:10.1177/0047287519855135

Watt, E. (2021). *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. Edward Elgar Publishing. doi:10.4337/9781789900101

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4). doi:10.5210/fm.v21i4.6161

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897. doi:10.1016/j.chb.2011.12.008

Wu, S. (2020). When new media operates within a state-mediated press system: Assessing new media's impact on journalism crisis perceptions in Singapore and Hong Kong. *Information Communication and Society*, *23*(4), 572–587. doi:10.1080/1369118X.2018.1521458

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, *19*(2–3), 137–149. doi:10.1007/s12525-009-0012-4

Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and Predicting Cyber Hacking Breaches. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2856–2871. doi:10.1109/TIFS.2018.2834227

Završnik, A. (2019). The European Digital Fortress and Large Biometric EU IT Systems: Border Criminology, Technology, and Human Rights. *Two Homelands*, *0*(49), 53–67. doi:10.3986/dd.v0i49.7253

Simon Vrhovec received the Ph.D. degree in computer and information science from the University of Ljubljana, Ljubljana, Slovenia, in 2015. He is currently an Associate Professor at the University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia. His main research interests include human factors in cybersecurity, software security engineering, agile methods, and change management. He has been in the steering committee of the European Interdisciplinary Cybersecurity Conference (EICC), since 2019, and co-chaired the Central European Cybersecurity Conference (CECC), in 2018 and 2019. He is an Editorial Board Member of the Journal of Cyber Security and Mobility (JCSANDM), Frontiers in Computer Science, EUREKA: Social and Humanities, and International Journal of Cyber Forensics and Advanced Threat Investigations (CFATI). He serves or has served as a Guest Editor for IEEE Security & Privacy, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), and Journal of Universal Computer Science (J.UCS).

Damjan Fujs is currently pursuing the Ph.D. degree with the Faculty of Computer and Information Science, University of Ljubljana, Slovenia. He is an Assistant with the Faculty of Computer and Information Science, University of Ljubljana. His research interests include cyber security, security requirements engineering, and software development methodologies. He has published in a range of scientific journals, such as Computers & Education, IEEE Access, and Journal of Universal Computer Science. Currently, he is or has been a member of the program committee of three conferences, namely, the Dnevi Slovenske Informatike (DSI 2022 and 2023), the International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2022 and 2023) and the European Interdisciplinary Cybersecurity Conference (EICC 2023).