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.

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

(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.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/are-perceptions-about-government-and-social-media-providers-related-to-protection-motivation-online/324085

Related Content

An Exploration of Digital Storytelling Creation and Media Production Skill Sets in First Year College Students
Scott Spicerand Charles Miller (2014). *International Journal of Cyber Behavior, Psychology and Learning (pp. 46-58).*
www.irma-international.org/article/an-exploration-of-digital-storytelling-creation-and-media-production-skill-sets-in-first-year-college-students/111135

A Systematic Review on Self-Construal and Social Network Sites
Soon Li Leeand Cai Lian Tam (2020). *International Journal of Cyber Behavior, Psychology and Learning (pp. 1-18).*
www.irma-international.org/article/a-systematic-review-on-self-construal-and-social-network-sites/255157

Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments
Eric D. Vugrinand Jennifer Turgeon (2014). *Cyber Behavior: Concepts, Methodologies, Tools, and Applications (pp. 2033-2055).*
www.irma-international.org/chapter/advancing-cyber-resilience-analysis-with-performance-based-metrics-from-infrastructure-assessments/107831

Teaching Online: The Handbook Dilemma in Higher Education
Tor Söderström (2011). *International Journal of Cyber Ethics in Education (pp. 10-21).*
www.irma-international.org/article/teaching-online-handbook-dilemma-higher/62635

Cyberbullying in Relation to Empathy and Friendship Quality
Redita Yuliawantiand Maria Goretti Adiyanti (2018). *International Journal of Cyber Behavior, Psychology and Learning (pp. 26-41).*
www.irma-international.org/article/cyberbullying-in-relation-to-empathy-and-friendship-quality/224012