The Relationship between Online Political Participation and Privacy Protection: Evidence from 10 Asian Societies of Different Levels of Cybersecurity

YU Wenting, SHEN Fei

Media and Communication, City University of Hong Kong, Hong Kong

*Email:feishen@cityu.edu.hk

City University of Hong Kong, Tat Chee Avenue, Kowloon Tong, Hong Kong.

The Relationship between Online Political Participation and Privacy Protection: Evidence from 10 Asian Societies of Different Levels of Cybersecurity

Information disclosure during online political activities can place participants under the threat of personal data leakage and misuse, but privacy protection in the context of online political participation has rarely been studied. This study examined how online political participation is related to privacy protection behaviors. Using survey data of internet users from 10 Asian societies, our study suggests two important findings. First, online political participation was found to be positively related to privacy protection behaviors. Second, we examined whether such a positive association can be explained by two mediators: perceived privacy risk and internet efficacy, in countries of different cybersecurity capacity. Our data suggest that internet efficacy mediates the relationship between online political participation and privacy protection behaviors across countries with different levels of cybersecurity capacity, while perceived privacy risk only mediates the effects of online political participation on privacy protection behaviors in countries of low cybersecurity capacity.

Keywords: internet use, political participation, privacy, cybersecurity, cross-nation

1.0. Introduction

Political participation helps express individual and community preferences, democratizes public decision-making, and facilitates efficient governance (Krishna, 2002; Przeworski, 1991). The proliferation of the internet lowers the cost of political participation (Bimber, 1999; Polat, 2005). Nowadays, the internet provides convenient access to a large variety of political activities, including but not limited to voting, petitions signing, and opinion expression (Bimber, 1999; Polat, 2005; Tolbert & McNeal, 2003).

However, at the same time, online political participation invites potential threats to personal privacy. People have to leave their personal information such as name, addresses, identity number, social security number, and credit card number on websites when they express opinions, vote, sign a petition, or make donations. The leak of these private information can constitute threats to one's personal, identity, and financial safety. Evidence shows that the confidentiality of these online data is questionable. Recently, U.S. voter information was exposed by a voter contact and canvassing app "Campaign Sidekick." An unprotected copy of the app's code was found mistakenly left publicly available online (Coker, 2020). In addition, quite a few countries around the world, the U.S. and the U.K. for example, run mass surveillance programs to collect a massive amount of citizen data from the internet (Ball et al., 2013), not to mention China's internet censorship and monitoring system.

The assurance of privacy is essential to motivating political participation. Privacy provides freedom of political expression and criticism, political choice, and avoiding unreasonable police interference (Akdeniz, 2002; Westin, 1968). If citizens face punishment when expressing their opinions or when voting for a preferred policy, they may hide their real thoughts or make involuntary political choices (Gavison, 1980; Heywood, 1997). Also, privacy concerns affect intention to participate. In 1990, residents in the U.S. were too afraid of privacy disclosure to respond to census survey mail (Singer et al., 1993). Today, as we are living in the "surveillance society" where government and corporates can easily access and analyze large personal information databases (Lyon, 2001), protecting one's privacy becomes more difficult and public demand for privacy protection grows rapidly (Burrus, 2015).

Therefore, privacy protection in online political participation is an important topic that deserves attention from scholars, human-right organizations, and policymakers.

Nevertheless, the protection of information privacy in the context of online political participation has rarely been studied. Most existing research on information privacy focuses on online commerce and social networking. In these contexts, privacy is conceptualized as a commodity as many studies found that individuals volunteer to exchange their privacy for benefits, such as sales discounts and attention from other social media users (Ellison et al., 2011; Xu et al., 2011; Youn, 2005). However, Knijnenburg et al. (2013) found that privacy disclosure behaviors are multidimensional, and thus scholars should not adopt a one-size-fits-all approach to it and should study privacy disclosure in different contexts. Privacy in online political participation is different from that in online commerce and social networking in terms of its importance and nature. First, privacy in online political participation motivates citizen self-governance and democratic policymaking (Akdeniz, 2002), while privacy in online commercial and social networking activities does not have the same social functions. Second, defining privacy as a commodity does not apply to the political context, since participants act to fulfill their political right, instead of obtaining material rewards or attention from social media. In online political participation, the definition of privacy is more close to the definition of general privacy: a basic human right (Smith et al., 2011).

This study aimed to explore how privacy protection behaviors are related to online political participation and the mechanisms behind it. We chose to contextualize our study in Asian societies for three reasons. First, internet use is rapidly developing in Asia. Internet penetration rate in Asia is growing rapidly from 21.5% in 2010 to 38.8% in 2015 and 55.1% in 2020 (Moore, 2020). By 2020, half of the world's internet population was in Asia (Internet World Stats, 2020). At the same time, the problem of online privacy violation becomes more salient and the need for privacy protection is increasing continuously(Privacy International, 2012). Second, Asian citizens face different levels of political freedom and governmental surveillance across countries since Asia has diverse types of political systems, including democracy (e.g., Japan), authoritarian regime (e.g., Singapore), and hybrid models (e.g., Hong Kong). Examining the effects of online political on privacy protection in a context with mixed political systems can lead to more comprehensive findings. Third, unlike European Union countries, Asian countries lack a comprehensive set of laws governing data privacy; instead, each country has its own privacy laws (Greenleaf, 2014; Marvin & Bowden, 2015), and the level of cybersecurity capacity varies (International Telecommunication Union, 2015). This study aims to examine the privacy protection and political participation across countries with different levels of cybersecurity capacity, and thus Asia's diversity of cybersecurity at the national level is a good fit for our purpose.

2.0. Literature Review

2.1. Online privacy protection behaviors

The discussion about online privacy is mostly referring to information privacy, which means the right to prevent the disclosure of personal information to others (Westin, 2003). Online privacy protection behaviors are individual actions for protecting one's online information from others, such as restricted use of location data, hiding profile information from other internet users, and giving false information to websites (Buchanan et al., 2007; Saeri et al., 2014).

Previous studies have mostly examined privacy protection behaviors within the contexts of online commerce and social networking. Those studies found a phenomenon called privacy paradox (Brown, 2001; Norberg et al., 2007), suggesting that people are worried about privacy infringement make little effort to protect their privacy. To explain why consumers voluntarily provide information online, many scholars recognize the economic component of privacy and conceptualize privacy as a commodity that can be traded

(Campbell & Carlson, 2002; Davies, 1997). Such a conceptualization is supported by empirical studies finding that consumers are willing to exchange privacy for material rewards or increasing influence in the social network (Acquisti, 2004; Ellison et al., 2011; Xu et al., 2011; Youn, 2005).

However, aside from being a commodity, privacy is also a basic human right in one's political and social life (Smith et al., 2011). Personal information disclosure not only happens to individuals as consumers but also to citizens in public deliberation. In Thailand, people concern about police intrusion and voting privacy more than consumer privacy (Privacy International, 2012). As the functions of the internet become more diverse, scholars suggest that we should not expect individuals to demonstrate the same behaviors in different contexts and thus more different online experiences should be explored in privacy research (Kokolakis, 2017; Xu et al., 2011). In other words, the patterns of online privacy protection should be examined in diverse contexts. In the past decade, an increasing number of studies examined online privacy protection in new contexts such as online healthcare services and location services (Acquisti & Gross, 2006; Al Ameen et al., 2012; Shokri et al., 2011). But to our best knowledge, no studies of privacy protection have been conducted in the context of political participation.

2.2. Online political participation and information disclosure

The proliferation of the internet increased the types and scale of political participation. E-participation tools such as e-panels, e-petitioning, and e-deliberative polling allow the public to express their opinions and engage in the process of policymaking (Aichholzer & Allhutter, 2011). In Asia, the young generations have shown a great passion for participating in online political activities (Center for Youth Studies, 2020; Chunly, 2019; Wike & Castillo, 2018).

Unfortunately, increased online political participation could lead to the disclosure of personal data. Individuals disclose personal data to websites when they vote, sign a petition, or make donations online, but websites can be compromised. For example, in 2013, a petition website Change.org, which had 35 million users in 196 countries at that time, was hacked (Almasy, 2013). Although the website claimed that the hacker only modified a petition and did not steal any personal information, the incident showed the vulnerability of third-party websites that collect sensitive user data. Later, a hacker stole more than 10,000 donors' data from a non-profit organization's website, including donors' names, addresses, contacts, and credit card information (McKellar, 2015).

Internet platforms with a large volume of user data can also compromise user privacy. The infamous Facebook-Cambridge Analytica scandal exposed in 2018 boosted public attention toward the privacy protection of social media. The incident involved Facebook data of 87 million people being used for election advertising (Tuttle, 2018). Regulators from different countries (e.g., U.S., Australia) sued Facebook for failing to protect individuals' data from unauthorized disclosure (BBC News, 2020; Youn, 2019).

Last but not least, governments could monitor user information for those who participate in politics. In authoritarian countries such as China, internet companies have to hand over user data to the government if they are required to do so (Kharpal, 2019). Information-based political manipulations happen in democratic societies as well. In 2013, Edward Snowden's exposure of mass surveillance by the U.S. National Security Agency triggered a heated discussion about online data and government surveillance (Lyon, 2014).

In conclusion, user privacy data generated through online political participation can be misused and abused by individuals, companies, and governments. Previous studies suggest that, in general, risky internet use is correlated with more privacy protection behaviors. Miline et al. (2004) found in an online survey that people who have bought from the web, provided email addresses to a website, and registered with a website in the recent past were more likely to take action to protect their online privacy. Chen et al. (2017) found that people

who have more experience in online shopping and opening emails from unknown sources are more likely to be victims of internet scam, and thus increase privacy protection actions. Some studies found that the use of social networking sites increased privacy concerns and motivated individuals to enhance privacy-setting strategies (Feng & Xie, 2014; Quinn, 2016). Based on the above evidence, it is reasonable to infer that online political participation, which can cause personal information disclosure, is positively associated with privacy protection behaviors. Therefore, we proposed the following hypothesis.

H1: Online political participation is positively related to privacy protection behaviors.

2.3. The role of perceived privacy risk

A more important question is: What drives people to take privacy protection measures in online political participation? To understand the mechanisms behind, we aim to explore the factors that connect online political participation with privacy protection.

A possible mediator is perceived privacy risk. According to Maslow's theory of motivation, humans act on safety needs in coping with external risks (Maslow, 1981). In other words, if people perceive privacy risk from online activities, they should act to protect themselves. Privacy risk includes the misuse of personal information due to insider disclosure or unauthorized access (Rindfleisch, 1997). Perceived privacy risk is the expectation of loss associated with the disclosure of personal data online (Xu et al., 2008), although some argue that people can get used to giving out private information to service providers and perceive less privacy risk as their online experience increases (Dai, 2007; Miyazaki & Fernandez, 2001).

When people engage in online political activities (e.g., online petitioning, voting), they have to provide personal information such as name, address, or even social security number. As a result, people who have more online political participation experiences should perceive more privacy risk. Researchers found that as people spend more time on the internet, they perceive higher risk of data leak and surveillance (Auxier et al., 2019; Consultancy.uk, 2018). Internet users are aware of the possible risk of online information disclosure, although they may not be able to link online activities with specific types of privacy risk (Gerber et al., 2019; Harbach et al., 2014; Karwatzki et al., 2017). Harbach, Fahl, and Smith's surveys (2014) in the U.S. and Germany found that most respondents can sense the risk of identity theft and abuse of information in online activities. A six-year longitudinal study of Facebook users found that perceived privacy risk increases rapidly among heavy users with time (Tsay-Vogel et al., 2016). Studies on the relationship between perceived privacy risk and privacy protection have shown different results. Some studies find evidence supporting the theory of privacy paradox, that perceived risk does not necessarily lead to more privacy protection (Debatin et al., 2009; Lee et al., 2013). However, more studies find that perceived risk is related to privacy protection behaviors. Norberge et al.'s study showed a positive correlation between risk perception and actual disclosure behaviors (2007). Using Facebook users data, Saeri et al. (2014) found that perceived privacy risk predicts intention to protect online privacy. Similarly, a study found that privacy risk perception lowers the intention of online disclosure and encourages protection behaviors (Keith et al., 2013).

Therefore, we hypothesized that in online activities, people should be able to identify privacy risks, which in turn motivates people to protect their privacy.

H2: Perceived privacy risk mediates the relationship between online political participation and privacy protection behaviors.

2.4. The role of internet efficacy

Another perception variable that could potentially mediate the relationship between online behaviors and privacy protection behaviors is internet efficacy. Self-efficacy is a crucial factor in social cognition (Bandura, 1998, 2010; Bandura & Adams, 1977). Eastin and

LaRose define internet efficacy as "the belief in one's capabilities to organize and execute courses of Internet actions required to produce given attainments, as a potentially important factor in efforts to close the digital divide that separates experienced Internet users from novices" (Eastin & LaRose, 2000, p. 1).

Bandura (1986) suggested that prior experiences can increase self-efficacy regarding the behaviors since people attribute their successful performances to personal abilities. For example, the experience of smoking cessation helps to improve people's self-efficacy of quitting smoking (Pardavila-Belio et al., 2019). Similarly, the experience of internet use increases internet efficacy. Eastin and LaRose (2000) found efficacy is positively correlated with internet use. Another study found that students who had more internet experience tend to have better self-perceptions about their abilities in using the internet for both exploration and communication (Tsai & Tsai, 2010). Later studies confirmed the positive effect of internet use experience on internet efficacy (Chuang et al., 2015; Kaya & Durmuş, 2010). Participating in online political activities involves internet experiences such as information searching, online communication, and using different websites. And thus, online political participation should also increase internet efficacy.

Meanwhile, people who possess high self-efficacy should exhibit more privacy protection behavior since efficacy motivates people to perform challenging tasks (Bandura & Adams, 1977). Also, protection motivation theory suggests that besides threat appraisal, self-efficacy as part of coping appraisal matters in motivating protection behaviors (Brouwers & Sorrentino, 1993; Maddux & Rogers, 1983). Empirical evidence showed that internet self-efficacy increases the technical protection of privacy via higher privacy concerns (Lee et al., 2017). Therefore, we hypothesize the following:

H3: Internet efficacy mediates the relationship between online political participation and privacy protection behaviors.

2.5. The role of cybersecurity capacity

Privacy perception and protection behavior show different patterns across societies. One study found that American respondents were less likely to restrict the visibility of their social network information than Chinese and Indians (Wang et al., 2011). Another study compared the specific privacy concerns in different countries, finding out that people from Europe are more concerned about data breaches than people from North America, and people from Asia and Europe believe that content and metadata are more critical than Americans do (Sheth et al., 2014).

Behavioral psychologists posited that behaviors are learned through interaction with the environment (Skinner, 1965). People learn new behaviors and adjust their current behaviors based on external conditions (Skinner, 1965). Internet use pattern varies across countries due to internet environmental factors, such as the levels of accessibility, privacy laws, and measures for internet governance (Greenleaf, 2014; Oderkirk et al., 2013; Wright et al., 2013). An analysis of Twitter users from more than 100 societies found that internet penetration is a significant predictor of privacy setting adoption and geolocation self-disclosure (Liang et al., 2016). Another study found that people from countries with government regulation of information privacy even desired more regulation than people from countries with no government regulation (Bellman et al., 2004; Milberg et al., 2000). A meta-analysis also suggested that the results of privacy studies varied across cultural orientation, and national legal systems (Baruh et al., 2017).

The current study aims to explore the influence of cybersecurity capacity at the national level on privacy protection behavior. Following the International Telecommunication Union (ITU), cybersecurity capacity in the current study is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can

be used to protect the cyber environment and organization and users' assets" (International Telecommunication Union, 2009, p. 2). In other words, countries with more advanced cybersecurity capacity can better protect user data from being stolen. A study comparing England and South Africa found that, although these two countries differ in cybersecurity capacity, people from the two countries both have high expectations for privacy protection (Da Veiga & Ophoff, 2020). But other cross-national studies found differences in privacy perceptions and behaviors in countries with different cybersecurity capacity. A study shows that students in the U.S., a country with a high level of cybersecurity capacity, are more cautious about presenting private information on social media, compared to students from India (Marshall et al., 2008). Also, the perception of risk is not independent of context (Reuter et al., 2019). Chen and Zahedi (2016) found a stronger association between perceived threat and privacy protection strategies in the U.S. than in China. They believed that the abuse of pirated software and the restricted knowledge of internet technologies in China made internet users more vulnerable to Internet security threats, and less confident in solving privacy problems on their own (Chen & Zahedi, 2016). In other words, a lack of cybersecurity capacity may provoke higher perceived privacy risk, lower internet efficacy, and less protection among internet users. Their conclusion can be explained by regression, a defense mechanism in psychology (Freud, 1937). Regression describes the phenomenon when people face great difficulties from the external environment, they give up coping with the situation with the skills they have; instead, they revert to an earlier stage of development (Freud, 1937). Based on these findings, we hypothesize that internet users will adjust their perceptions and privacy protection behaviors in response to the external cybersecurity environment.

H4: The mediation effects of perceived privacy risk vary across societies of different national cybersecurity.

H5: The mediation effects of internet efficacy vary across societies of different national cybersecurity.

3.0. Methods

3.1. Data

The fieldwork was contracted out to YouGov, an international polling company with a proprietary panel that covers Europe, the U.S., the Middle East, and Asia-Pacific. The data are from a multinational survey of internet users in Asia conducted between August 1 and August 24 in 2015, and the average response rate was 12.72%. In total, 6,691 respondents finished the survey and passed the quality check. The survey finally collected data from 10 Asian societies: Hong Kong (n = 631), India (n = 1,000), Indonesia (n = 600), Japan (n = 600), Malaysia (n = 779), Pakistan (n = 600), Singapore (n = 600), South Korea (n = 600), Thailand (n = 633), and Vietnam (n = 648). The choice of these countries was based on three considerations. The first consideration was the cultural and economic representativeness of Asia. The selected countries represent Confucianism, Buddhism, Muslim, Hinduism, and other Asian cultures. Also, the selected countries cover both developed (i.e., Hong Kong, Japan, Singapore, and South Korea) and developing areas (i.e., India, Indonesia, Malaysia, Pakistan, Thailand, and Vietnam). Second, since this study investigates the effects of online political participation, the levels of internet freedom should be considered. Based on the world internet freedom index developed by Free House (Freedom House, 2015), we planned a balanced distribution among free (i.e., Hong Kong, Japan, and South Korea), partly free (i.e., India, Indonesia, and Malaysia), and not free (i.e., Pakistan, Singapore, Thailand, and Vietnam) countries. Last but not least, we considered the diversity of cybersecurity capacity. Based on the Global Cybersecurity Index that adopts a 0-1 scale (International

Telecommunication Union, 2015), the selected countries range from 0.18 (i.e., Pakistan) to 0.77 (i.e., Malaysia) on cyber cybersecurity capacity. In the same year, the country that ranked first on the cybersecurity scale was the U.S., scoring 0.82.

Since this study focuses on internet users rather than the general population, quota sampling based on gender, age, education, and income distribution of the internet user population in each country was used. The statistics of internet user profiles were mostly collected from the government statistical bureau in 2015. For countries that do not provide statistics on internet users, we relied on overall demographic feature statistics.

3.2. Measures

Privacy protection behaviors. Some studies operationalize information disclosure as a reversed measure of privacy protection (Saeri et al., 2014; Young & Quan-Haase, 2013). However, a study found that Twitter users who have more privacy protection settings show more self-disclosure (Liang et al., 2016). It seems that these two concepts should not be treated as the opposite of each other. Hence, we asked whether respondents have taken the given nine strategies to protect their online privacy in the past 12 months. The sum of these nine dummy variables (1= yes, no =0) formed the index of privacy protection behaviors (M = 4.52, SD = 2.32, α = .72). We listed the 9 protection behaviors and the number of respondents who have taken them in the past 12 months as follows: "used a separate password for sensitive data" (n = 5349, 72.7%), "set sharing permission for friends and family only" (n = 4799, 65.2%), "read the privacy policies of websites or services that you share personal information with" (n = 4782, 65.0%), "restricted use of location data by websites or apps" (n = 4686, 63.7 "downloaded a web browser plug-in"(n = 3879, 52.7%), "reused throw-away password for low-value accounts"(n = 3536, 48.1%), %), "provided incorrect data (e.g., fake name, date of birth) when creating a new account" (n = 2413, 32.8%), "tried to make sure your identity was protected online using anonymization tools (for example, TOR, etc.)"(n = 1963, 37.2%), and "tried to secure your email and instant messaging communication using encryption tools (e.g., Chatsecure, ProtonMail.)"(n = 1836, 25.0%). These protection behavioral indicators were chosen based on previous studies (Chen et al., 2017; Park et al., 2012; Youn & Hall, 2008; Young & Quan-Haase, 2013).

Perceived privacy risk. The items for measuring perceived privacy risk were adapted from previous literature (Dinev & Hart, 2004). The index was created by taking the average scores of the following two items: "personal information I submit online could be made available to third parties without my knowledge." and "personal information I submit online could be inappropriately used." Respondents were asked to rate these items on a 5-point Likert scale, from 1 "strongly disagree" to 5 "strongly agree" (M = 3.27, SD = 1.19, α = .84).

Online political participation. Online political participation measured the number of political activities respondents performed in the past 12 months. The items were adapted from the World Value Survey (Inglehart et al., 2014), which include "sign a petition online," "contacted a national, state, or local government official online," "contributed money online for political or social causes," "send a 'letter to the editor' to a newspaper or magazine online." The average of the four items formulates an index (M = 1.04, SD = 1.26, α = .69).

Internet efficacy. Internet self-efficacy was measured by two items adapted from previous studies (Eastin & LaRose, 2000). Respondents are asked to rate the extent to which they agree with the statements on a 5-point scale (1= "strongly disagree" and 5 = "strongly agree"): "I feel confident finding the information I want on the internet." and "I feel confident troubleshooting internet problems." The average of the two items formulates an index (M = 3.47, SD = .77, α = .66).

Cybersecurity capacity. We used the 2015 Global Cybersecurity Index (GCI) to operationalize cybersecurity (*Global Cybersecurity Index & Cyberwellness Profiles*, 2015). The ITU leads the research of GCI to raise awareness of the importance of cybersecurity

globally. GCI assesses 193 nation's cybersecurity in terms of legal, technical, organizational, capacity building, and cooperation perspectives. The legal measures include criminal legislation as well as regulation and compliance. The technical measures include computer incident response team, standards, and certification. The organizational measures include policy, roadmap for governance, responsible agency, and national benchmarking. Capacity building includes standardization development, manpower development, professional certification, and agency certification. Cooperation measures include intra-state cooperation, intra-agency cooperation, public-private partnerships, and international cooperation. Nations were rated on a continuous scale from 0 to 1, where 1 indicates high security. Societies rated lower than 0.5 on GCI were categorized as societies with low cybersecurity capacity, including Thailand, Vietnam, Indonesia, and Pakistan. Societies rated higher than 0.5 on GCI were classified as societies with high cybersecurity capacity, including Hong Kong, Singapore, Korea, Japan, India, and Malaysia.

Control variables. Previous studies suggest that an individual's demographic profiles (i.e., gender, age, income, and education) affect one's privacy perceptions and behaviors, and thus they enter the model as control variables (Hoffmann et al., 2015; Kokolakis, 2017; Marwick et al., 2017; Youn & Hall, 2008). Gender is a dummy variable where females were coded as 0 and males as 1. The sample includes 50.8% males and 49.2% females. Age is an ordinal variable with six categories ranging from "below 20" to "60 and above" (M = 2.96, SD = 1.13). The school system varies across different societies, but we created a uniform 4-level education indicator: secondary school or below (35.3%), vocational college education (40.6%), college or university (19.3%), and post-graduate degree (7.8%). Income brackets also differ in different countries. Therefore, standardized income scores were calculated within each country and then used for analysis.

3.3. Data analysis

We tested the multiple mediation model using PROCESS, Model 4 (Hayes, 2012), with age, gender, education, and income as control variables. Assessment of the multiple mediation models involved an analysis of the total and specific indirect effects (Preacher & Hayes, 2008). In our analysis, the parameter estimates and confidence intervals of the total and specific indirect effects were based on 5,000 random samples. To examine how much variance in the dependent variable was explained by each predictor, we report the results of regression analyses predicting privacy protection behaviors, perceived privacy risk, and internet efficacy, respectively.

In addition, we aim to test the same model for societies with different levels of cybersecurity. With the data collected from different societies, the ideal is to conduct multilevel modeling, which is used for analyzing data with a cluster structure. However, some scholars argue that when the number of units at the second level is small, using MLM can cause biased estimates of the second-level standard errors. Snikders and Bosker (2012) suggest a minimum of 20 clusters for multilevel modeling. Based on a simulation study, Maas and Hox pointed out that executing multilevel modeling with 50 or fewer units at a higher level is inappropriate (Maas & Hox, 2005). This study only collected data from 10 societies, which did not meet the ideal qualification for multilevel modeling. Alternatively, we categorized the 10 countries into two groups, high and low cybersecurity capacity, and examined the model separately.

4.0. Results

The means and standard deviations of privacy protection behaviors, online political participation, perceived privacy risk, and internet efficacy are listed by countries in the Appendix.The regression results predicting privacy protection behaviors, perceived privacy risk, and internet efficacy at the individual level using data from all countries are shown in Table 1. Before formal hypotheses testing, we report the effects of control variables on

privacy protection behaviors. Based on findings from Model 1 in Table 1, males (beta =*.05*, $p < .001$) were more likely to take privacy protection actions than females. Individuals that were younger (beta =-.22, $p < .001$), had higher levels of education (beta =.11, $p < .001$), and had higher income (beta =.06, $p < .001$) reported more privacy protection behaviors.

Table 1. Predicting privacy protection behaviors, perceived privacy risk, and internet efficacy in all countries and areas ($N = 6691$).

	Privacy protection behaviors				Perceived privacy risk		Internet efficacy	
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8
Gender	.05***	.02	.02	.01	.01	.00	.09***	.07***
Age	-.22***	-.18***	-.18***	-.16***	.08***	.09***	-.12***	-.10***
Income	.06***	.03***	.03**	.02	-.09***	-.10***	.10***	.09***
Education	.11***	.08***	.08***	.07***	.06***	.06***	.08***	.07***
OPP[a]		.35***	.35***	.33***		.05***		.16***
PPR[b]			.03**					
Efficacy				.13***				
R^2(%)	6.2***	18.3***	18.4***	19.9***	1.4***	1.6***	3.6***	5.8***

Note: OPP[a] refers to "online political participation", and [b]PPR refers to "perceived privacy risk.

We reported the standardized coefficient in OLS regression results.

** $p < .01$, *** $p < .001$.

Also, before we formally tesed our hypotheses with data at individual level, we performed the correlations between the examined variables at the national level (see Figure 1) for robustness checking. There was a positive correlation between online political participation, privacy protection behaviors, and internet efficacy. But online political participation showed a negative association with perceived privacy risk.

[Figure 1 about here]

Next, we tested our hypotheses. Hypothesis 1 posited a positive relationship between online political participation and privacy protection behaviors. The hypothesis was supported by statistics (beta =.35, $p < .001$). Online political participation explained about 12.1% of the variance in privacy protection (see Model 2 in Table 1).

[Figure 2 about here]

Then we proceeded to mediation analysis. Results of Model 3 and 6 in Table 1 showed that online political participation was positively related to perceived privacy risk (beta =.05, $p < .01$), but perceived privacy risk was not significantly related to privacy protection behaviors (beta =.02, $p = .12$). The results suggest that the mediation effect of perceived privacy risk on the relationship between online political participation and privacy protection behaviors were not statistically significant (standardized effect = .001, 95%*CI* [-.000, .001]). In other words, Hypothesis 2 was not supported.

In contrast, internet efficacy (standardized effect = .020, 95%*CI* [.016, .025]) was a significant mediator of the relationship between online political participation and privacy protection behaviors, which supported Hypothesis 3. Results of Model 4 and 8 showed that online political participation was positively related to internet efficacy (beta =.16, $p < .001$), and internet efficacy was positively related to privacy protection behaviors (beta =.13, $p < .001$, increased R^2 =1.6%). The effects of online political participation on privacy protection behaviors remained significant after internet efficacy was introduced to the model (see Model 4 in Table 1). Hence, the coefficient of the mediation effect by internet efficacy

was significant. Figure 2 visualized the path and results of the mediation effects tested in the full dataset.

Last, we examined H4 and H5, that the mediation effects vary across societies with different levels of cybersecurity. We first examined the mediation models in countries with a high level of cybersecurity, and the results of regression models are shown in Table 2. Online political participation was positively related to privacy protection behaviors (beta =.38, $p < .001$), according to the results of Model 10. The coefficient of online political participation predicting privacy protection bahaviors decreased after introducing the mediators into the model (beta =.35, $p < .001$). Thus we continue to test if the mediation effects were statistically significant. It turns out that the mediation effects of perceived privacy risk were not significant (standardized effect = .001, 95%*CI* [-.000, .002]). But the mediation effects of internet efficacy were significant (standardized effect = .029, 95%*CI* [.022, .036]). The effects of the mediation models for countries with a high level of cybersecurity are visualized in Figure 3.

Table 2. Predicting privacy protection behaviors, perceived privacy risk, and internet efficacy in countries with high cybersecurity ($N = 4210$).

	Privacy protection behaviors				Perceived privacy risk		Internet efficacy	
	Model 9	Model 10	Model 11	Model 12	Model 13	Model 14	Model 15	Model 16
Gender	.04*	.00	.00	-.01	-.00	-.01	.08***	.06***
Age	-.23***	-.18***	-.18***	-.16***	.02	.03	-.15***	-.12***
Income	.10***	. 05**	.05**	.03*	-.02	-.02	.15***	.12***
Education	.09***	. 05**	.04***	.04*	.04	.04*	.07***	.05**
OPP[a]		.38***	.38***	.36***		.04**		.20***
PPR[b]			.02					
Efficacy				.15***				
R^2(%)	7.2***	21.0***	21.1***	22.9***	2.0***	4.0***	5.8***	9.5***

Note: Countries and areas with high cybersecurity include Hong Kong, Singapore, Korea, Japan, India, and Malaysia.

OPP[a] refers to "online political participation", and [b]PPR refers to "perceived privacy risk.

We reported the standardized coefficients in OLS regression results.

*p <.05, ** p <.01, *** p <.001.

For countries with a low level of cybersecurity, the regression results predicting privacy protection behaviors, perceived privacy risk, and internet efficacy are shown in Table 3. Again, online political participation had a significant and positive relationship with privacy protection behaviors (beta =.26, $p < .001$), based on the results of Model 17. The coefficient of online political participation predicting privacy protection behaviors decreased after introducing the mediators into the model (beta =.25, $p < .001$). Thus we continue to test if the mediation effects were significant in countries with a low level of cybersecurity. Perceived privacy risk (standardized effect = .005, 95%*CI* [.002, .010]) was found to be a significant mediator. Besides, internet efficacy (standardized effect = .004, 95%*CI* [.001, .009]) partially mediated the relationship between online political participation and privacy protection behaviors. The mediation effects of perceived privacy risk and internet efficacy were not significantly different, 95%*CI* [-.007, .009]. The effects of the mediation models for countries with a low level of cybersecurity are visualized in Figure 4.

[Figure 4 about here]

Table 3. Predicting privacy protection behaviors, perceived privacy risk, and internet efficacy in countries with low cybersecurity (N = 2481).

	Privacy protection behaviors				Perceived privacy risk		Internet efficacy	
	Model 17	Model 18	Model 19	Model 20	Model 21	Model 22	Model 23	Model 24
Gender	.05*	.03	.03	.03	.03	.02	.08***	.08***
Age	-.14***	-.14***	-.15***	-.14***	.12***	.12***	-.01	-.01
Income	.06**	.04*	.06**	.04***	-.26***	-.27***	.05*	.05*
Education	.12***	.12***	.12***	.12	.05*	.05*	.04***	.04
OPP[a]		.26***	.26***	.26***		.09***		.06**
PPR[b]			.07***					
Efficacy				.08***				
R^2(%)	3.0***	11.3***	11.8***	12.0***	7.6***	8.4***	1.0***	1.4***

Note: Countries with low cybersecurity include Thailand, Vietnam, Indonesia, and Pakistan.
OPP[a] refers to "online political participation", and [b]PPR refers to "perceived privacy risk.
We reported the standardized coefficient in OLS regression results.
*p <.05, ** p <.01, *** p <.001.

The results showed that the effects mediated by perceived privacy risk was significant in countries with low levels of cybersecurity but not significant in countries with high levels of cybersecurity. Therefore, H4 was supported. Furthermore, we compared the mean scores of perceived privacy risk in countries with high and low levels of. Results showed that people from countries with high cybersecurity capacity (M = 3.35, SD = 1.15) perceived more privacy risk than people from countries with low cybersecurity capacity (M = 2.97, SD = 1.32), and the difference was significant (t = -12.09, p < .001).

Internet efficacy mediated the relationship between online political participation and privacy protection behaviors in countries with both high and low levels of cybersecurity. For a formal test, we performed a Fisher's Z test across two datasets following Cohen et al. (2013). Results showed that the difference was not significant, Z = .10, p = .32. Thus, H5 was not supported by our data.

5.0. Discussion and Conclusion

This study tackles three main questions by analyzing survey data from 10 Asian countries. First, we investigated to what extent Asian people adopt privacy protection behaviors in the context of online political participation. Second, we explored the mediators linking online political participation to privacy protection behaviors, examining the phenomenon of privacy paradox. And third, we examined how the factor of the external environment – cybersecurity, affects the mediation effects. The findings of this study not only shed light on online privacy research, but also provide suggestions for government, political parties, and NGOs in terms of guiding citizens to protect their privacy rights.

First, this study found that online political participation was an important predictor of online privacy protection, which explained about 12.1% percent of the variance in privacy protection behaviors. Also, online political participation was positively correlated with perceived privacy risk. In other words, people who are active in online political participation are aware of the potential risk of privacy disclosure and will take more privacy protection actions. While existing studies that mostly focus on privacy protection in online commerce and conceptualize privacy as a commodity, this study argues that internet use in the political context also motivates privacy protection behaviors. Moreover, the conceptualization of online privacy should be reconsidered. In a political context, online privacy is not a

commodity but a basic human right, and thus privacy protection in online political participation can be considered as behaviors protecting personal rights. Governments, political parties, and NGOs should be more careful about privacy protection in online political activities if they want to motivate citizen engagement in democratic policymaking.

Second, we examined the mediation effects of perceived privacy risk between online political participation and privacy protection behaviors. Analyzing data from all countries, online political participation was positively related to perceived privacy risk, but perceived privacy risk did not have a significant effect on privacy protection behaviors, which is consistent with the phenomenon of privacy paradox (Brown, 2001; Norberg et al., 2007).

However, the correlation between perceived privacy risk and privacy protection behaviors showed different patterns in countries with high and low levels of cybersecurity separately. Only in countries with less cybersecurity capacity, perceived privacy risk had a significant impact on privacy protection, and the impact was positive. In other words, perceived privacy risk lead to privacy protection behaviors in countries with a low level of cybersecurity, but not in countries with a safer internet environment. Is this because people from countries with higher levels of cybersecurity perceive less privacy risk? Figure 1 suggests the opposite: countries with a higher level of cybersecurity generally show a higher level of perceived privacy risk. Comparing the mean value of perceived privacy risk between countries with high and low level of cybersecurity also suggest that a higher level of cybersecurity does not necessarily ease people's perception of online privacy risk. But only a riskier cyber environment can turn perceived privacy risk into actual protection behaviors. Our findings did not support Chen and Zahedi's assumption that people in a more risky internet environment feel overwhelmed to deal with the threats (Chen and Zahedi, 2016). Instead, for internet users from countries with less cybersecurity capacity, risk perception is more likely to lead to actual privacy protection.

The results provide a plausible explanation for the inconsistent findings of the privacy paradox in previous studies. That is, the phenomenon of privacy paradox might only appear in societies with a higher level of cybersecurity. People from countries with high cybersecurity capacity may rely more on solutions at the societal/national level to ease their risk perception, while those from countries with low cybersecurity capacity tend to rely on themselves to protect their online privacy. Existing studies are mostly conducted in developed countries (e.g., the U.S.), therefore, it is important to study privacy protection in regions with low cybersecurity capacities, such as South America, Africa, and the underdeveloped countries in Asia based on the latest ITU assessment (International Telecommunication Union, 2018).

Third, compared to perceived privacy risk, internet efficacy is a more robust and stable mediator linking online political participation to privacy protection. No matter in countries with a more secure or riskier cyber environment, online political participation was associated with internet efficacy, which led to more privacy protection behaviors. However, it should be noted that the magnitude of the effects differs across countries with high and low levels of cybersecurity capacity. The correlation between online political participation and perceived privacy risk, and that between perceived privacy risk and privacy protection behaviors are higher in countries with securer cyber environments. We speculate that in a country with well-developed policies and technologies for online privacy protection, citizens can better obtain skills and literacy from their online activities. In addition, people from high-security environments are usually better educated about privacy protection and their knowledge motivates them to prevent themselves from potential risks, while people living in countries with low cybersecurity capacity are more likely to act in response to perceived risks.

The findings of the mediation effects offer some practical implications as to how to increase peoples' privacy protection behaviors. First, fear appeal seems to be useful in countries with a lower level of cybersecurity. Second, it is always important to increase people's internet efficacy. Previous studies found knowledge as an important predictor of internet efficacy (Rimal, 2000). Hence, educating people on privacy protection strategies should be useful in motivating them to take privacy protection actions.

It is important to point out the limitations of this study. First, it should be noted that both perceived privacy risk or internet efficacy only partially mediated the effects of online political participation on privacy protection behaviors, and the mediation effects were moderate. Hence, the mechanisms connecting online political participation and privacy protection behaviors require further examination. Second, we examined 10 Asian societies in this study and these societies might not be representative of all Asian countries. In particular, China as an important Asian country is not included in this study due to the difficulty of collecting survey data on political participation and circumvention tool use in China. It is highly possible that as a country with severe internet censorship, the relationships between the variables we examined could be different. Third, with cross-sectional survey data, we are not able to ascertain the causal directions of the relationships we examined. The arguments we made about causality are purely based on theoretical speculations. Besides, survey data can only investigate self-reported instead of actual behaviors. Studies examining actual behaviors of privacy protection in experimental settings should be more valuable.

References

Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification* In *Proceedings of the 5th ACM conference on electronic commerce* (pp. 21-29).

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer, Berlin, Heidelberg.

Aichholzer, G., & Allhutter, D. (2011). *Online forms of political participation and their impact on democracy*. Verlag d. Österr. Akad. d. Wiss.

Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research: An International Quarterly, 69*(1), 223-237.

Akhter, S. H. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing*. https://doi.org/10.1108/JCM-06-2013-0606

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93-101. https://doi.org/10.1007/s10916-010-9449-4

Almasy, S. (2013, 27 May). Hackers hit petition site Change.org, official says. *CNN Bussiness*. https://edition.cnn.com/2013/05/26/tech/change-website-hacked/index.html

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Ball, J., Borger, J., & Greenwald, G. (2013, 6 September). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Bandura, A. (1986). Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy. https://doi.org/10.1037/0003-066X.41.12.1389

Bandura, A. (1998). Personal and collective efficacy in human adaptation and change. *Advances in Psychological Science, 1*, 51-71.

Bandura, A. (2010). Self-efficacy. *The Corsini encyclopedia of psychology*, 1-3. https://doi.org/10.1002/9780470479216.corpsy0836

Bandura, A., & Adams, N. E. (1977). Analysis of self-efficacy theory of behavioral change. *Cognitive Therapy and Research, 1*(4), 287-310. https://doi.org/10.1007/BF01663995

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. https://doi.org/10.1111/jcom.12276

BBC News. (2020, 9 March). Cambridge Analytica: Australia takes Facebook to court over privacy. *BBC News*. https://www.bbc.com/news/technology-51799738?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-scandal&link_location=live-reporting-story

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324. https://doi.org/10.1080/01972240490507956

Bimber, B. (1999). The Internet and citizen communication with government: Does the medium matter? *Political Communication, 16*(4), 409-428. https://doi.org/10.1080/105846099198569

Brouwers, M. C., & Sorrentino, R. M. (1993). Uncertainty orientation and protection motivation theory: The role of individual differences in health compliance. *Journal of Personality and Social Psychology, 65*(1), 102. https://doi.org/10.1037/0022-3514.65.1.102

Brown, B. (2001). *Studying the Internet experience*. HP laboratories technical report HPL, Issue.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165. https://doi.org/10.1002/asi.20459

Burrus, D. (2015). The privacy revolt: The growing demand for privacy-as-a-sevice. *Wired*, *3*. https://www.wired.com/insights/2015/03/privacy-revolt-growing-demand-privacy-service/

Campbell, J. E., & Carlson, M. (2002, 2002/12/01). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586-606. https://doi.org/10.1207/s15506878jobem4604_6

Center for Youth Studies. (2020). *"Youth political participation and social media use in Hong Kong" research report*. http://youthstudies.com.cuhk.edu.hk/survey-results

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291-302. https://doi.org/10.1016/j.chb.2017.01.003

Chen, Y., & Zahedi, F. M. (2016). Individuals'internet security perceptions and behaviors: polycontextual contrasts between the united states and china. *MIS Quarterly, 40*(1). https://doi.org/10.25300/MISQ/2016/40.1.09

Chuang, S.-C., Lin, F.-M., & Tsai, C.-C. (2015, 2015/07/01/). An exploration of the relationship between Internet self-efficacy and sources of Internet self-efficacy among Taiwanese university students. *Computers in Human Behavior, 48*, 147-155. https://doi.org/10.1016/j.chb.2015.01.044

Chunly, S. (2019, 2019/10/02). Facebook and political participation in Cambodia: determinants and impact of online political behaviours in an authoritarian state. *South East Asia Research, 27*(4), 378-397. https://doi.org/10.1080/0967828X.2019.1692635

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge. https://doi.org/10.4324/9780203774441

Coker, J. (2020, 21 March). *Sensitive Voter Data Exposed by App Use in US Elections*. https://www.infosecurity-magazine.com/news/voter-data-exposed-app-us-elections/

Da Veiga, A., & Ophoff, J. (2020). Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa. In N. Clarke & S. Furnell, *Human Aspects of Information Security and Assurance* (pp. 16-29). Springer, Cham.

Davies, S. G. (1997). Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. *Technology and Privacy: The New Landscape, 143*, 144.

Dai, B. (2007). *The impact of online shopping experience on risk perceptions and online purchase intentions: the moderating role of product category and gender* (Doctoral dissertation).

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-*

Mediated Communication, 15(1), 83-108. https://doi.org/:10.1111/j.1083-6101.2009.01494.x

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422. https://doi.org/10.1080/01449290410001715723

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of Computer-Mediated Communication, 6*(1), JCMC611. https://doi.org/10.1111/j.1083-6101.2000.tb00110.x

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy online* (pp. 19-32). Springer. https://doi.org/10.1007/978-3-642-21521-6_3

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33*, 153-162. https://doi.org/10.1016/j.chb.2014.01.009

Freedom House. (2015). *Freedom on the net*. https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf

Freud, A. (1937). *The ego and the mechanisms of defence*. L. and Virginia Woolf at the Hogarth Press, and the Institute of psycho-analysis.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal, 89*(3), 421-471. https://doi.org/10.2307/795891

Gerber, N., Reinheimer, B., & Volkamer, M. (2019). Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies, 2019*(3), 267-288. https://doi.org/10.2478/popets-2019-0047

Global Cybersecurity Index & Cyberwellness Profiles. (2015). International Telecommunication Union. Retrieved 22 August from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

Greenleaf, G. (2014). *Asian data privacy laws: trade & human rights perspectives*. OUP Oxford.

Harbach, M., Fahl, S., & Smith, M. (2014, 19-22 July 2014). Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *2014 IEEE 27th Computer Security Foundations Symposium* (pp. 97-110). IEEE. https://doi.org/10.1109/CSF.2014.15

Hayes, A. F. (2012). *PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling [White paper]*.

Heywood, A. (1997). *Politics*. Macmillan.

Hoffmann, C. P., Lutz, C., & Meckel, M. (2015). Content creation on the Internet: A social cognitive perspective on the participation divide. *Information, Communication & Society, 18*(6), 696-716. https://doi.org/10.1080/1369118X.2014.991343

Inglehart, R., Haerpfer, C., Moreno, A., Welzel, C., Kizilova, K., Diez-Medrano, J., Lagos, M., Norris, P., Ponarin, E., & Puranen, B. (2014). World values survey: Round six-country-pooled datafile version. *Madrid: JD Systems Institute.*

International Telecommunication Union. (2009). *Overview of Cybersecurity*. International Telecommunication Union. Retrieved August 22 from http://www.itu.int/rec/T-REC-X.1205-200804-I/en

International Telecommunication Union. (2015). *Global cybersecurity index & cyberwellness profiles*. http://handle.itu.int/11.1002/pub/80c63097-en

International Telecommunication Union. (2018). *Global Cybersecurity Index (GCI)*. International Telecommunication Union. Retrieved 22 August from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Internet World Stats. (2020). *Internet Usage in Asia*. Retrieved 15 December from https://www.internetworldstats.com/asia.htm

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017, 2017/11/01). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems, 26*(6), 688-715. https://doi.org/10.1057/s41303-017-0064-z

Kaya, S., & Durmuş, A. (2010, 2010/01/01/). Pre-service teachers' perceived internet self-efficacy and levels of internet use for research. *Procedia - Social and Behavioral Sciences, 2*(2), 4370-4376. https://doi.org/10.1016/j.sbspro.2010.03.695

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. https://doi.org/10.1016/j.ijhcs.2013.08.016

Kharpal, A. (2019, 4 March). Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. *CNBC*. https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013, 2013/12/01/). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies, 71*(12), 1144-1162. https://doi.org/10.1016/j.ijhcs.2013.06.003

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

Krishna, A. (2002). Enhancing Political Participation in Democracies:What is the Role of Social Capital? *Comparative Political Studies, 35*(4), 437-460. https://doi.org/10.1177/0010414002035004003

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862-877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Lee, W. Y., Tan, C.-S., & Siah, P. C. (2017). The Role of Online Privacy Concern as a Mediator between Internet Self-Efficacy and Online Technical Protection Privacy Behavior. *Sains Humanika, 9*(3-2).

Liang, H., Shen, F., & Fu, K.-w. (2016). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society, 19*(9), 1476-1497. https://doi.org/10.1177/1461444816642210

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education (UK).

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714541861

Maas, C. J. M., & Hox, J. J. (2005). Sufficient Sample Sizes for Multilevel Modeling. *Methodology, 1*(3), 86-92. https://doi.org/10.1027/1614-2241.1.3.86

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9

Marshall, B. A., Cardon, P. W., Norris, D. T., Goreva, N., & D'Souza, R. (2008). Social networking websites in India and the United States: A cross-national comparison of online privacy and communication. *Issues in Information Systems, 9*(2), 87-94. https://doi.org/10.48009/2_iis_2008_87-94

Marvin, L. M., & Bowden, Y. (2015). Conducting US Discovery in Asia: An Overview of E-Discovery and Asian Privacy Laws. *Richmond Journal of Law & Technology, 21*(4), 12.

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society, 3*(2), 2056305117710455. https://doi.org/10.1177/2056305117710455

Maslow, A. H. (1981). *Motivation and personality*. Prabhat Prakashan.

McKellar, K. (2015, 29 August). *Utah Food Bank security breach exposed thousands of donors' info since October, 2013*. https://www.databreaches.net/utah-food-bank-security-breach-exposed-thousands-of-donors-info-since-october-2013/

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science, 11*(1), 35-57. https://doi.org/10.1287/orsc.11.1.35.12567

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

Moore, M. (2020). *Internet penetration rate in Asia compared to the global penetration rate from 2009 to 2020*. https://www.statista.com/statistics/265156/internet-penetration-rate-in-asia/

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Oderkirk, J., Ronchi, E., & Klazinga, N. (2013, Sep). International comparisons of health system performance among OECD countries: opportunities and data privacy protection challenges. *Health Policy, 112*(1-2), 9-18. https://doi.org/10.1016/j.healthpol.2013.06.006

Pardavila-Belio, M. I., Canga-Armayor, A., Duaso, M. J., Pueyo-Garrigues, S., Pueyo-Garrigues, M., & Canga-Armayor, N. (2019). Understanding how a smoking cessation intervention changes beliefs, self-efficacy, and intention to quit: a secondary analysis of a pragmatic randomized controlled trial. *Translational Behavioral Medicine, 9*(1), 58-66. https://doi.org/10.1093/tbm/ibx070

Park, Y. J., Campbell, S. W., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior, 28*(3), 1019-1027. https://doi.org/10.1016/j.chb.2012.01.004

Polat, R. K. (2005). The Internet and political participation: Exploring the explanatory links. *European Journal of Communication, 20*(4), 435-459. https://doi.org/10.1177/0267323105058251

Preacher, K. J., & Hayes, A. F. (2008). Contemporary approaches to assessing mediation in communication research. In A. F. Hayes, M. D. Slater, & L. B. Snyder (Eds.), *The Sage sourcebook of advanced data analysis methods for communication research*. Sage.

Privacy International. (2012). *A new dawn: Privacy in Asia*. https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf

Przeworski, A. (1991). *Democracy and the market: Political and economic reforms in Eastern Europe and Latin America*. Cambridge University Press.

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media, 60*(1), 61-86. https://doi.org/10.1080/08838151.2015.1127245

Reuter, C., Kaufhold, M. A., Schmid, S., Spielhofer, T., & Hahne, A. S. (2019). The impact of risk cultures: Citizens' perception of social media use in emergencies across Europe. *Technological Forecasting and Social Change*, *148*(1), 1-17. https://doi.org/10.1016/j.techfore.2019.119724

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, 40(8), 92-100. https://doi.org/10.1145/257874.257896

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014, Jul-Aug). Predicting Facebook users' online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior. *Journal of Social Psychology, 154*(4), 352-369. https://doi.org/10.1080/00224545.2014.914881

Sheth, S., Kaiser, G., & Maalej, W. (2014). Us and them: a study of privacy requirements across north america, asia, and europe. Proceedings of the 36th International Conference on Software Engineering - ICSE 2014,

Shokri, R., Theodorakopoulos, G., Le Boudec, J.-Y., & Hubaux, J.-P. (2011). Quantifying Location Privacy. *2011 IEEE Symposium on Security and Privacy*, 247-262. https://doi.org/10.1109/sp.2011.18

Singer, E., Mathiowetz, N. A., & Couper, M. P. (1993). The impact of privacy and confidentiality concerns on survey participation the case of the 1990 U.S. census. *Public Opinion Quarterly, 57*(4), 465-482. https://doi.org/10.1086/269391

Skinner, B. F. (1965). *Science and human behavior*. Simon and Schuster.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989-1015. https://doi.org/0.2307/41409970

Tolbert, C. J., & McNeal, R. S. (2003). Unraveling the effects of the Internet on political participation? *Political Research Quarterly, 56*(2), 175-185. https://doi.org/10.1177/106591290305600206

Tsai, M.-J., & Tsai, C.-C. (2010, 2010/05/01/). Junior high school students' Internet usage and self-efficacy: A re-examination of the gender gap. *Computers & Education, 54*(4), 1182-1192. https://doi.org/10.1016/j.compedu.2009.11.004

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2016). 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. https://doi.org/10.1177/1461444816660731

Tuttle, H. (2018). Facebook scandal raises data privacy concerns. *Risk Management*, *65*(5), 6-9. http://www.rmmagazine.com/2018/05/01/facebook-scandal-raises-data-privacy-concerns/.

Wang, Y., Norice, G., & Cranor, L. F. (2011). *Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites* Berlin, Heidelberg.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453. https://doi.org/10.1111/1540-4560.00072

Wike, R., & Castillo, A. (2018). *Many around the world are disengaged from politics, but could be motivated to participate on issues like health care, poverty and education*. https://www.pewresearch.org/global/2018/10/17/international-political-engagement/

Wright, D., Finn, R., & Rodrigues, R. (2013). A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research, 9*(1). https://doi.org/10.1007/978-94-007-2543-0_1

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110. https://doi.org/10.1207/s15506878jobem4901_6

Youn, S. (2019, 24 July). US regulators fine Facebook $5 billion for privacy claims; sue Cambridge Analytica. *abc News*. https://abcnews.go.com/Business/us-regulators-fine-facebook-billion-settle-privacy-claims/story?id=64533218

Youn, S., & Hall, K. (2008, Dec). Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior, 11*(6), 763-765. http://doi.org/10.1089/cpb.2007.0240

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society, 16*(4), 479-500. https://doi.org/10.1080/1369118x.2013.777757

Appendix. Descriptive data of privacy protection behaviors, online political participation, perceived privacy risk, and internet efficacy by countries.

	M	*SD*
Privacy protection behaviors		
Hong Kong	4.82	2.04
Singapore	3.93	2.34
Korea	3.86	2.44
Japan	2.38	2.14
India	5.13	2.31
Malaysia	1.70	2.30
Thailand	4.82	2.29
Vietnam	5.13	2.03
Indonesia	1.02	1.25
Pakistan	4.22	1.55
Online political participation		
Hong Kong	0.97	1.23
Singapore	0.68	1.04
Korea	0.68	1.08
Japan	0.19	0.59
India	1.65	1.42
Malaysia	0.99	1.23
Thailand	0.86	1.29
Vietnam	1.04	1.21
Indonesia	1.02	1.25
Pakistan	2.02	0.92
Perceived privacy risk	3.67	0.76
Hong Kong		
Singapore	0.68	1.04
Korea	3.55	1.14
Japan	3.79	0.74
India	3.16	1.25
Malaysia	3.17	1.18
Thailand	3.85	0.76
Vietnam	2.75	1.38
Indonesia	2.21	1.24
Pakistan	3.03	1.24
Internet efficacy	3.45	0.65
Hong Kong		
Singapore	3.40	0.70
Korea	3.26	0.75
Japan	2.96	0.82
India	3.80	0.78
Malaysia	3.49	0.72
Thailand	3.55	0.72
Vietnam	3.59	0.84
Indonesia	3.62	0.63
Pakistan	3.43	0.83